Director, Operational Test and Evaluation

FY 2016 Annual Report

December 2016

This report satisfies the provisions of Title 10, United States Code, Section 139. The report summarizes the operational test and evaluation activities (including live fire testing activities) of the Department of Defense during the preceding fiscal year.

J. Michael Gilmore
Director

FY 2016
Annual Report

Introduction

I have served as the Director, Operational Test and Evaluation at the request of the President and Congress since September 2009. It has been an honor and a privilege to serve in this position for over seven years. During my confirmation, I pledged to assure that all of the Department's acquisition systems under my oversight undergo rigorous operational and live fire test and evaluation to determine whether they are operationally effective, suitable, and survivable. I also pledged to provide meaningful, credible test results on system performance to the Congress and civilian and military leaders so that they could make informed decisions regarding acquisition and employment of those systems. In my final annual report to Congress, I review the accomplishments of this office over my tenure, the challenges that the T&E community continues to face, and the consequences of repeatedly fielding equipment that cannot be counted on in combat – a trend that will continue unless rigorous independent operational testing is conducted early and adequately on all systems.

At the core of my pledge to ensure rigorous testing and credible results has been the use of scientific and statistical approaches to realistic operational test design and analysis starting at the beginning of a system's development. The test community has made enormous progress in increasing the use of scientific test design, increasing statistical rigor and improving the analytical capabilities of the Department of Defense (DOD) workforce. The National Research Council recommended the use of modern statistical techniques in defense test and evaluation in 1998, but these techniques were not fully embraced by the operational test community until I provided the direction and implementation guidance early in my tenure. The use of statistical test and analysis techniques is now standard procedure at all of the Operational Test Agencies (OTAs) and is similarly supported by the DOD's developmental test and evaluation office.

Implementation of rigorous test design and analysis provides defensible, factual information to support critical roles of this office. The topics below illustrate how my office has implemented rigorous test design, independent oversight, and objective analysis to support the DOD acqusition system:

- Data to support rapid fielding
- Opportunities for early problem discovery
- Rationales for not conducting testing
- Meaningful, testable requirements and test measures
- Rationales for test adequacy
- Efficient test plans that cover the operational envelope
- Characterization of performance across the operational envelope
- Optimum use of scarce resources
- Improved understanding of system usability
- Methodologies for cybersecurity testing and analysis
- Design for reliability
- Methodologies for combining data from multiple tests
- Rigorous validation of models and simulations
- Improved test resources for evolving threats

The remainder of this introduction summarizes some of the most critical impacts of this office over my tenure. Examples illustrate the value of our products to our primary customer, the soldiers, airmen, sailors, and marines who must ultimately use these systems to accomplish their missions.

IMPROVEMENTS IN TEST AND EVALUATION

The primary goal of operational testing is to understand how new and upgraded systems will perform under the stresses of realistic combat conditions, prior to the Full-Rate Production decision and fielding to combat units. Understanding the capabilities and limitations of systems before they are used in combat is important to commanders in the field and to the men and women who protect our country. Furthermore, the identification of problems permits corrective action before large quantities of a system are procured and minimizes expensive retrofitting of system modifications. Even for systems in which a few units (e.g., ships, satellites) will be acquired, operational testing is essential to find and fix problems, which often can only be found in operationally realistic test conditions, and characterize system performance across operational conditions before the warfighter has to use it in combat.

Rapid Fielding

One of my first priorities as Director was to support rapid fielding of new capabilities to meet urgent needs on the battlefields in Iraq and Afghanistan. My office relied on the use of all available data to provide information regarding performance of these systems. Since 2009, we have published more than 20 early fielding reports to Congress on critical combat systems such as countermeasures for helicopters, small form fit radios, air-to-ground munitions, and many naval systems including ship self-defense missiles, torpedo warning systems, and both variants of the Littoral Combat Ship (LCS). These reports identified performance problems that were either fixed before deployment or made known to the combatant commanders and joint forces that depended on them.

Early Problem Discovery

My office has advocated for earlier realistic testing and problem discovery so that acquisition decision makers can make timely decisions. The Undersecretary of Defense for Acquisition, Technology and Logistics' (USD(AT&L)) 2016 report on the defense acquisition system described $58 Billion in sunk costs over the last two decades on programs that were ultimately canceled. While this figure includes 22 major programs such as the Army's Future Combat System and Comanche Helicopter, it does not include other major programs developed outside the primary acquisition system such as the Airborne Laser and Air Force transformational satellites. To help avoid expensive programs continuing in development while not delivering military utility, my office now requires operational assessments (OAs) for all programs be conducted prior to the Milestone C production decision, when problem discoveries may highlight significant mission shortfalls and problems are cheaper to fix.

Early testing (both developmental test events and OAs) should inform the development process and enable the early identification of major problems. More than just providing an early opportunity for problem detection, an OA provides a chance to build knowledge on how the system will perform once placed in an operational environment. The use of Design of Experiments (DOE), even in early testing, allows efficient test designs that cover the operational envelope. Knowledge gained from OAs can help refine the resources necessary for the IOT&E, such as the most significant factors affecting operational performance, potentially reducing the scope for the IOT&E. In ideal cases, the use of sequential test design from early testing including OAs through IOT&E can provide even more efficient use of test budgets by combining information across test phases. While my office has successfully integrated information from OAs and IOT&Es, integrated developmental and operational testing is the exception and not the rule. One challenge in particular is having production-representative articles early enough to do realistic tetsing.

Rapid Realistic Testing Improves Design and Saves Lives: Mine Resistant Ambush Protected (MRAP)

Mine Resistant Ambush Protected (MRAP) vehicles are a family of vehicles designed to provide increased crew protection against battlefield threats, such as Improvised Explosive Devices (IEDs), mines, and small arms. Because of the urgent operational need for increased crew protection against battlefield threats in Iraq and Afghanistan, multiple MRAP vehicle configurations had to be procured, tested, and fielded on a highly accelerated basis.

DOT&E supported rapid, but operationally realistic testing. The MRAP Joint Program Office originally planned to conduct live fire testing against only Key Performance Parameter (KPP) threshold level of explosive underbelly and side attack threats. However, these KPP-level threats were smaller than known threats in the planned theaters of operation. Consequently, DOT&E required testing against larger explosive threats consistent with those documented in combat.

DOT&E worked with the Army and the Marine Corps to rapidly plan and conduct this testing, which revealed not only significant vulnerabilities against larger, more operationally realistic threats, but also revealed stark differences between the crew protection provided by the different MRAP variants as the threat sizes increased. Despite resistance from the Army, DOT&E immediately reported these newly discovered vulnerabilities and performance differences to the Department leadership and commanders in the field, leading the Program Office to develop, test, and implement design changes that could be retrofitted onto vehicles in theater as well as built into future production lines. The Army and the Marine Corps also considered these differences when selecting the MRAP variants they would retain in their enduring fleet. These timely reports resulted in equipment modifications and tactics changes that likely saved lives of American and Allied soldiers.

Conduct Operational Test Only when Systems are Ready

Having a clear understanding of the required testing provides a rationale for making decisions on when operational tests will or will not provide value to the community. While my office has been a strong supporter of OAs prior to Milestone C, operational testing should only be conducted when appropriate. In cases where systems are clearly not ready for rigorous, realistic testing, we have recommended against spending scarce resources to observe poor performance. Instead, DOT&E has advocated that those resources be reallocated to address capability shortfalls. In the case of the Remote Multi-Mission Vehicle (RMMV), my office recommended that the Navy cancel a planned OA because of well-documented reliability problems. We instead recommended that the Navy dedicate the resources allocated for the OA towards making improvements to the Increment 1 mine countermeasures (MCM) mission package. (See details in reliability section.)

My office also recommended the cancelation of the Army Integrated Air and Missile Defense (AIAMD) Limited User Test (LUT) in favor of a developmental test because of well-known problems with an immature system that was falling well short of performance requirements to demonstrate readiness for a Milestone C production decision. The LUT proceeded against our recommendation, but evaluated less than one-third of the effectiveness measures because of system immaturity and the lack of readiness of some AIAMD capabilities. As DOT&E predicted, the LUT was adequate to confirm poor effectiveness, poor suitability, and poor survivability. My office recommended that the Army fix all critical deficiencies and conduct another LUT to demonstrate the full range of capabilities identified in the May 2012 Test and Evaluation Master Plan (TEMP) under operationally realistic and system stressing conditions.

Early Problem Discovery:
CVN 78 USS *Gerald R. Ford*

CVN 78 is the lead ship in the Navy's newest class of aircraft carriers. USS *Gerald R. Ford* is scheduled to be delivered in 2017. The design incorporates several new systems including a new nuclear power plant, weapons elevators, radar, catapult, and arresting gear.

In the last two CVN 78 OAs, DOT&E examined the reliability of new systems onboard CVN 78 and noted that the poor or unknown reliability of the Electromagnetic Aircraft Launch System (EMALS), the Advanced Arresting Gear (AAG), the Dual Band Radar (DBR), and the Advanced Weapons Elevators (AWE) is the program's most significant risk to successful use in combat. These systems affect major areas of flight operations – launching aircraft, recovering aircraft, air traffic control, and ordnance movement. DOT&E noted that unless these reliability problems are resolved, which would likely require redesigning AAG and EMALS, they will significantly limit CVN 78's ability to conduct combat operations.

CVN 78 is intended to support high-intensity flight operations. The CVN 78 Design Reference Mission (DRM) specifies a 35-day wartime scenario. The DRM includes a 4-day surge with round-the-clock flight operations and 270 aircraft sorties per day. The DRM also includes 26 days of sustained operations with flight operations over a nominal 12 hours per day and 160 aircraft sorties per day.

Based on AAG reliability to recover aircraft, CVN 78 is unlikely to support high-intensity flight operations. AAG has a negligible probability (<0.0001 percent) of completing the 4-day surge and less than a 0.2 percent chance of completing a day of sustained operations without an operational mission failure.

EMALS has higher reliability than AAG, but its reliability to launch aircraft also is likely to limit flight operations. EMALS has less than a 7 percent chance of completing the 4-day surge and a 67 percent chance of completing a single day of sustained operations without a critical failure.

DBR's unknown reliability for air traffic control and ship self-defense is a risk to the IOT&E and for combat operations. The Program Office does not have a DBR reliability estimate based on test data. Because CVN 78 will be delivered soon and DBR hardware is already installed in the ship, it will be difficult to address any significant reliability issues should they arise.

Canceling the F-35 Joint Strike Fighter (JSF)
Block 2B Operational Utility Evaluation

When asked in 2012 whether the Services supported the need for the Block 2B Operational Utility Evaluation (OUE), both the Air Force and the Navy stated that they would consider using the F-35 Block 2B aircraft in combat and hence required the testing planned for the Block 2B OUE.

In March 2014, I recommended not conducting the planned F-35 Block 2B OUE, scheduled for the summer of 2015 to evaluate the "initial warfighting capabilities" of the F-35A and F-35B aircraft. My recommendation was based on observations that the program was behind schedule in completing the Block 2B development, and the OUE would only delay the necessary progression to Block 3F development, which is needed to complete development and begin IOT&E. I predicted that the results of the OUE would confirm what we already knew – that the Block 2B F-35 would be of limited military utility. Also, there was substantial evidence that the aircraft would not be ready to support training of operational pilots and successful completion of a comprehensive operational evaluation. The USD(AT&L) and the JSF Program Executive Officer agreed with my recommendation, and the JSF Operational Test Team refocused their efforts from conducting the OUE to activities that would help the program progress toward completing Block 2B, and eventually Block 3F development.

Meaningful, Testable Requirements and Test Measures

My office has continually engaged with the requirements community in efforts to improve requirements and in doing so helped numerous programs refine their requirements early in the acquisition cycle, thereby saving time and resources from trying to achieve the unobtainable. We have pointed out unrealistic reliability requirements in programs like ground combat vehicles, tactical datalinks, and long-range air defense radars; these programs were able to establish the rationale for lower thresholds for providing desired mission performance.

The initial reliability requirement for the Joint Light Tactical Vehicle (JLTV) of 4,500 Mean Miles Between Operational Mission Failure (MMBOMF) was much larger than comparable systems such as the High Mobility Multi-purpose Wheeled Vehicle (HMMWV), and would have been very difficult to achieve. Based on feedback from my office and other stakeholders on what reliability is practically achievable and necessary to support mission objectives, user representatives reduced the requirement to 2,400 MMBOMF. This requirement has a clear, mission-based rationale and is verifiable within a reasonable operational test period.

Early engagement also helps programs write requirements in such a manner that they are testable within a reasonable timeframe. We have encouraged the use of continuous metrics such as time, distance, and accuracy in place of binomial metrics such as probability of hit or probability of kill in order to reduce the testing required to confidently demonstrate compliance with requirements. Additionally, even in cases where requirements are not updated, the Service OTAs have now made it common practice to use continuous metrics to scope the operational test in addition to evaluating the required hit/kill-type requirements.

We continue to observe, that while necessary, Key Performance Parameters (KPPs) are not sufficient for testing military systems. KPPs often lack the context of the complex operational environment, including current threats. A few examples:

- P-8A Poseidon is a maritime patrol aircraft that will replace the P-3C Orion and conduct anti-submarine warfare (ASW) and other missions. However, the KPPs required only that the P-8A be reliable, be equipped with self-protection features and radios, and carry a requisite number of sonobuoys and torpedoes, but not actually demonstrate an ability to find and prosecute submarines. DOT&E, working with the Navy's OTA, focused the testing on examining quantitative mission-oriented measures, beyond the limited KPPs, in order to characterize the aircraft's ASW capabilities.
- *Virginia*-class submarine is a multi-mission nuclear attack submarine that is replacing the existing *Los Angeles*-class submarine. During the IOT&E, the submarine failed to meet two KPP thresholds. However, *Virginia's* performance was equivalent to or better than the legacy *Los Angeles*-class in all mission areas, leading my office to evaluate the *Virginia* as operationally effective and operationally suitable.
- Early Infantry Brigade Combat Team (EIBCT) systems were a collection of sensors the Army planned to use in infantry brigades to detect and provide warning of enemy activities. The KPPs for some of the sensors specified only that the systems produce images recognizable as human faces at specified distances—not an expected detection range or a probability of detection. DOT&E advocated and the Army agreed that the systems be tested under realistic combat conditions against a capable enemy threat, which revealed that enemy soldiers could easily spot the large antennas needed to transmit the images back to the operations centers. Additionally, many of the sensors were not useful to soldiers even though they met the KPPs. As a result, the Army canceled the portions of the program that were unnecessary.

As these examples clearly illustrate, operational context is necessary to fully evaluate systems, whether they meet their KPPs or not. My office continues to work with requirements organizations to ensure requirements are achievable, testable, and operationally meaningful, but some independent evaluation metrics will always be necessary, especially in the case of evolving threats.

Writing Measurable Requirements: Air and Missile Defense Radar (AMDR)

The Navy's new SPY-6 Air and Missile Defense Radar (AMDR) is intended to provide an improved Integrated Air and Missile Defense (IAMD) capability to the next flight of USS *Arleigh Burke* (DDG 51) class destroyers (i.e. DDG 51 Flight III). In 2012, DOT&E reviewed the Navy's draft Capability Development Document for AMDR. DOT&E's review noted that several of the program's requirements, including its IAMD Key Performance Parameter (KPP), were probabilistic in nature and would require an unachievable amount of operational testing. Verifying the IAMD KPP, for example, would have required hundreds of ballistic missile and anti-ship cruise missile surrogates. To improve the testability of the AMDR KPPs, DOT&E provided the Navy with alternative metrics using continuous variables like time and range for assessing the radar's capability. The Navy ultimately adopted metrics similar to those suggested by DOT&E, reducing required testing while maintaining the desired capability.

Defensible Rationales for Test Adequacy

Throughout my tenure I have emphasized that the statistical approaches of Design of Experiments (DOE) provide a defensible and efficient methodology for not only determining test adequacy but also ensuring that we obtain the maximum value from scarce test resources. DOE has proven to elicit maximum information from constrained resources, provided the ability to combine information across multiple independent test events, and produced defensible rationale for test adequacy and quantification of risk as a function of test size.

One clear advantage of statistical approaches to evaluating test adequacy is that they provide a means to quantify how much information can be derived from each test point. Clearly, the first time a projectile is fired at a helmet and does not penetrate we learn something new. The second, third, and fourth times, we learn about the robustness of that helmet and whether the first result was a fluke or a consistent trend. But if we fire 10 projectiles at 10 helmets, what is the value of firing the 11th projectile? As the test progresses, we are incrementally not learning as much as the first shot. Statistical methods provide a quantitative trade-space for identifying that point of diminishing returns and also the associated risks of making incorrect decisions based on limited test sizes. My office and the Service OTAs have found these methods invaluable when debating the cost/benefit of additional test points.

Efficient Test Plans that Cover the Operational Envelope

A critical aspect of operational testing is identifying how system capabilities are challenged when placed in operationally realistic conditions. However, today's modern systems are not only designed to contribute to multiple mission areas, but also work across a wide range of operational conditions. The constantly evolving threat further complicates the challenge of determining not only how much testing is enough, but also the conditions under which we need to test. My office has successfully used DOE to address how much testing is needed and also to select points that efficiently span the operational space to ensure that we have a complete picture of performance.

Statistically Rigorous Test Protocols: Enhanced Combat Helmet (ECH)

It is critical that we ensure that the protective equipment we provide to our soldiers meets the high quality that is demanded. After I was asked to assume oversight of personnel protective equipment, I directed that testing of these systems follow protocols that were comparable to existing statistically-based industry quality control methodologies. Employing a statistical approach allowed the Department to set quantifiable quality standards.

Those standards proved valuable following an engineering change proposal intended to increase manufacturing capacity for the ECH. The ECH failed the small arms component of the DOT&E-approved protocol. The helmet failed because of too many small arms penetrations, which demonstrated that the helmet did not provide the desired protection. The manufacturer ultimately decided it was necessary to use different ballistic shell laminate material to provide for an acceptable helmet against the small arms threat.

Designing an Efficient Test for a Multi-Mission Strike Fighter

The F-35 is a multi-role fighter aircraft being produced in three variants for the Air Force, Marine Corps, and Navy. The multi-dimensional operational space created by the mission types, aircraft variants, ground and air threats, and weapons loads is very complex, yet suited for the use of experimental design to efficiently ensure adequate coverage of the operational space for characterizing the performance of the F-35 in all mission areas. Additionally, experimental design enables a "matched pairs" construct for doing comparison testing between the F-35 and the legacy aircraft it is replacing.

The overarching test approach for the F-35 Block 3F IOT&E was to create detailed test designs for evaluating each of the core mission areas by defining appropriate, measurable response variables corresponding to operational effectiveness of each mission area. The test team divided the operational space – using DOE concepts – into factors that would affect the response variables, e.g., type of ground threat or number and types of red air threat, and varied those factors to ensure coverage of the operational space in which the F-35 may be used in combat. Also, the test team sought to maximize information collection by dividing the threat continuum into categories and then assigning coverage to the appropriate mission areas. The team also ensured that key capabilities would be assessed in at least one mission area. For example, finding, tracking, and engaging moving ground targets are enabled by the ground moving target indicator (GMTI) and ground moving target track (GMTT) functions of the radar, and are only covered in strike coordination and reconnaissance and close air support (CAS) missions. This allowed the test team to assess GMTI and GMTT capability without including moving ground targets in all of the mission areas.

The application of DOE to the test design process also supports the development of objective comparison tests. One of the purposes of operational testing is to provide realistic and objective assessments of how systems improve mission accomplishment compared to previous systems under realistic combat conditions. The F-35 requirements document states that the F-35 will replace legacy aircraft, including the A-10, in the CAS mission, so the test design includes a comparison test of the F-35A and the A-10 in this role.

Optimum Use of Scarce Resources

DOE and corresponding statistical analysis methods have supported extracting the maximum value from scarce test resources in a defendable manner. In cases where testing is expensive and there is pressure to reduce test sizes, DOE allows us to understand up front what information we are giving up. Additionally, these methods can assist in finding holes in our current knowledge and placing test points so that they provide the greatest information gain.

Improved Understanding of System Usability

A key aspect of operational testing is observing the quality of human-systems interactions and their impact on mission accomplishment. Operators are a critical component of military systems. Hardware and software alone cannot accomplish missions. Systems that are too complex for operators to use compromise mission success by inducing system failures and force the Services to invest in lengthy and expensive training programs to mitigate problems that arise because of poor interface design. DOT&E has provided guidance on the best practices of the use of surveys in operational test and evaluation

KC-130J Harvest Hercules Airborne Weapon Kit (HAWK)

The Navy is updating the Harvest HAWK that allows the KC-130J tanker/mobility aircraft to employ HELLFIRE and Griffin laser-guided missiles for close air support. Under an Urgent Operational Need Statement, Harvest HAWK has been deployed in theater since 2010 without a formal operational test. The updated Harvest HAWK includes a new sensor for targeting weapons and for laser designation and a new mission operator station. The Navy proposed a limited operational test with only a few end-to-end demonstrations of live munitions. My office proposed a more robust test design based on current tactics documents and munition capabilities. The Navy rejected that proposal, claiming that the system was adequately proven in combat and only limited testing was needed. The Navy provided the available combat data and our analysis showed that while the munitions generally perform well, there are significant gaps between where the system has been used in combat and the desired capabilities of the updated system. The combat data provided significant information on performance during the day, at one altitude, and against stationary targets. Very little information was available on different altitudes, at night, and against moving targets. The Navy is now working with my office to update the operational test design to collect the data that are necessary to fill those gaps.

Long Range Anti-Ship Missile (LRASM)

My office received a request from the Navy to reduce the number of free-flight test shots for the LRASM quick reaction assessment because of budget limitations. The Navy proposed reducing the number of weapons from the previously agreed upon 12 missiles to 6. The proposed reduction excluded important aspects of the operational engagements that looked at different target ranges and aspect angles, which I believe could affect the success rate and performance of the missile.

I was also concerned with having limited live testing to validate the modeling and simulation (M&S) tool. As it stands, the planned 12-shot free-flight program, provides limited opportunity to validate the M&S. Executing any less would not provide adequate information to detect differences between free-flight testing and the M&S. As a direct result, we would run the risk of mischaracterizing the performance of the weapon across the operational test space.

Through statistical analysis techniques, I determined the 12 missiles provided a minimally adequate test for assessing weapon performance and validating the M&S integral to this quick reaction capability. Therefore, I would not approve a test strategy with less than this minimum.

The Navy accepted this analysis and my decision.

Warfighter Information Network – Tactical (WIN-T) Usability Concerns

Original Interface (complex) New Interface (Simplified)

WIN-T is an Army communications system using both satellite and terrestrial datalinks. It allows soldiers to exchange information in tactical situations.

The initial testing of WIN-T focused on its technical performance. Testing revealed not only poor technical performance, but also problems with the complexity of the system. Even when the software and hardware were properly functioning, soldiers found the system difficult to operate. Usability has been a key concern as WIN-T has since been upgraded over the years.

Subsequent testing focused on improvements to the man/machine interface that soldiers use to operate the system on the battlefield. As depicted above, the original interface was complex and difficult to read. The interface had multiple sub-menus and when the system failed, it could take 40 minutes to an hour to restart it. The new interface is far simpler.

Testers used surveys to evaluate the difficulties that soldiers had when using the system. The Army initially constructed surveys that were complex, with nested questions and "Not Applicable" as a potential response. DOT&E encouraged the test and evaluation community to incorporate survey science into the testing, and worked with the Army to improve the surveys. The revised surveys are simpler, more meaningful, more likely to be completed reliably, and easier to interpret. Well-designed surveys allow operational evaluations to rigorously incorporate the soldiers' experience and are crucial for DOT&E evaluations and reporting to Congress.

to critically evaluate the usability of military systems as well as the workload, fatigue, and frustration that operators experience while employing the system. Surveys are often the only means to evaluate these issues; proper scientific survey design must be done to ensure that the data collected to evaluate the quality of human-system interactions are valid and reliable.

Methodologies for Cybersecurity Testing and Analysis

Improving our understanding of the cyber threat, including recognizing that cybersecurity applies to more than automated information systems, and improving the rigor of cyber testing rigor have been two of my office's more notable achievements. Most military systems, networks, and missions are susceptible to degradation as a result of cyber-attacks. DOT&E evaluates the cybersecurity posture of units equipped with systems and live DOD networks during operational testing and Combatant Command and Service exercises. Important efforts include our continued emphasis on identifying how cybersecurity affects operational missions, inclusion of cyber defenses in tests, improvement of Red Team skills, and analytical methodologies and measures. We have also advocated for overarching cyber assessments that focused on identifying cross-cutting problems for the Department to address. In 2014, I published comprehensive guidance to the OTAs, updating and reinforcing guidance we have been using since Congress directed DOT&E perform annual evaluations of Combatant Command and Service cybersecurity postures in 2002. The DOD acquisition process should deliver systems that provide secure and resilient cyber capabilities; therefore, operational testing must examine system performance in the presence of realistic cyber threats. My 2014 guidance specifies that operational testing should include a cooperative vulnerability and penetration assessment phase to identify system vulnerabilities followed by an adversarial assessment phase to exploit vulnerabilities and assess mission effects. My guidance encourages program managers to address cybersecurity vulnerabilities that are discovered during the cooperative vulnerability and penetration assessment, prior to conducting the adversarial assessment. Despite this, adversarial assessments often find exploitable mission-critical vulnerabilities that earlier technical testing could have mitigated.

My office continues to emphasize the need to assess the effects of a debilitating cyber-attack on the users of DOD systems so that we understand the impact to a unit's mission success. A demonstration of these mission effects is often not practicable during operational testing due to operational safety or security reasons. I have therefore advocated that tests use simulations, closed environments, cyber ranges, or other validated and operationally representative tools to demonstrate the mission effects resulting from realistic cyber-attacks. Representative cyber environments hosted at cyber ranges and labs provide one means to accomplish the above goals. Such cyber ranges and labs provide realistic network environments representative of warfighter systems, network defenses, and operators, and they can emulate adversary targets and offensive/defensive capabilities without concern for harmful effects to actual in-service systems/networks. For several years, I have proposed enhancements to existing facilities to create the DOD Enterprise Cyber Range Environment (DECRE), which is comprised of the National Cyber Range (NCR); the DOD Cybersecurity Range; the Joint Information Operations Range; and the Joint Staff J-6 Command, Control, Communications, and Computers Assessments Division. The need and use of these resources is beginning to outpace the existing DECRE capabilities. As an example, the NCR experienced a substantial increase in customers the last few years.

Cybersecurity continues to evolve rapidly as both new threats and new defensive capabilities emerge and are fielded. Our ability to test and evaluate the DOD's cyber posture must keep pace with these advancements by accelerating development of appropriate tools and techniques. For example, Programmable Logic Controllers (PLCs) are ubiquitous in both fixed installations and deployable platforms, such as ships and aircraft. DOT&E has provided guidance on the necessity for caution in testing these components due to risk of platform damage caused by a PLC that is compromised, and has invested in the development of safe test and evaluation techniques for PLCs. Test agencies must continue to use all available tools and resources to assess PLCs and other industrial control systems used in DOD platforms. Other cybersecurity test challenges include:

- Systems with non-Internet Protocol data transmission (e.g., Military Standard 1553 data bus)
- Multiple Spectrum Cyber Threats (e.g., via non-computer based networks)
- Customized attacks
- End-to-end testing to include key subsystems, peripherals, and plug-ins
- Cloud computing

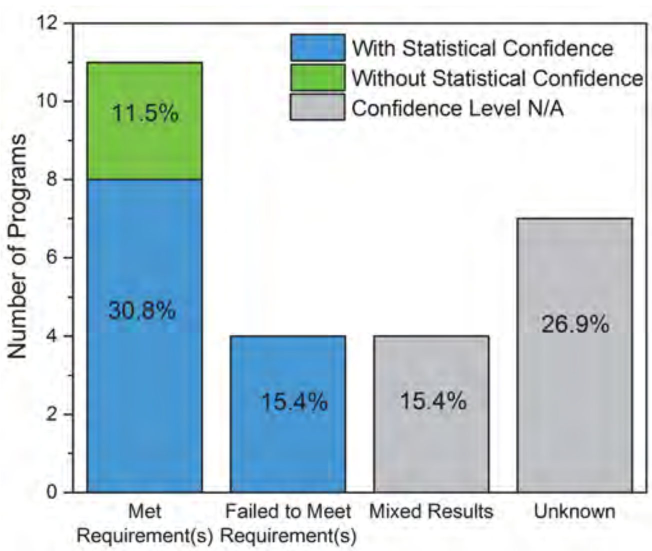
The Services' OTAs have established a cybersecurity technical exchange forum to discuss ongoing challenges and share solutions and lessons learned to improve overall cybersecurity operational test process. There were two meetings this year, which also included DOT&E participation. These interchanges are a good step forward for the operational test community to keep pace with the threat.

Design for Reliability

I similarly made improvement of system reliability a top priority – through initial design and early testing rather than discovering shortfalls at the end of development in operational testing. In my office's evaluation of oversight programs, we continue to see rising compliance with the policies set forth in the DODI 5000.02 and DOT&E guidance memos. The use of reliability growth curves as a tool to monitor progress of a system's reliability is now standard practice. The most successful programs are incorporating reliability growth into their contracts and have reliability thresholds as KPPs

However, change takes time and, despite the Department's continued efforts to emphasize the importance of reliability, defense systems continue to demonstrate poor reliability in operational testing. Only 11 of 26 systems (42 percent) that had a post-Milestone C operational test in FY16 met their reliability requirements. The remaining 15 systems either failed to meet their requirements (15 percent), met their requirements on some (but not all) parts of the overall system of systems (15 percent), or could not be assessed because of limited test data or the absence of a reliability requirement (27 percent).

Analysis of these recent operational tests indicates that one of the challenges in demonstrating whether a system meets its reliability requirement in operational testing is planning a long enough test. While tests are generally not scoped with respect to the reliability requirement, sufficient data should be captured throughout all testing phases to determine the reliability of the system as it compares to the requirements. The operational test scope for many systems is not long enough to demonstrate reliability requirements with statistical confidence. Over the past 3 years, 13 percent of requirements have planned test lengths shorter than the requirement itself. For systems with high reliability requirements, it is particularly important to intelligently use test data from all available sources. When system reliability is poor, even a short test might be adequate to prove the system did not meet its reliability requirement.



DISTRIBUTION OF RELIABILITY RESULTS FOR POST-MILESTONE C TESTING IN FY16 (UNKNOWN RESULTS INDICATE EITHER NOT ENOUGH DATA TO EVALUATE OR NO RELIABILITY REQUIREMENT)

Methodologies for Combining Data from Multiple Tests

While rigorous operational testing is paramount to this office's assessment of operational effectiveness, suitability, and survivability, it is not always possible or practical to obtain all of the information required for our assessments in an operational test. My office has supported the use of all information in operational evaluations in order to provide the best assessments available and use test resources in the most responsible fashion. In recent guidance updates, we have provided a pathway for using developmental test data in operational evaluations. We have enthusiastically advocated for considering all of the information available in reliability assessments.

Rigorous Validation of Modeling and Simulation (M&S)

Another focus area we are just beginning to influence is the rigorous validation of M&S that are to be used in the evaluation of a system's combat effectiveness and suitability. I expect the validation of M&S to include the same rigorous statistical and analytical principles that have become standard practice when designing live tests. All M&S, when used to support

Elements of a Successful Reliability Growth Program: Joint Light Tactical Vehicle (JLTV)

The JLTV is a partial replacement for the High Mobility Multi-purpose Wheeled Vehicle (HMMWV) fleet. The JLTV program presented a unique opportunity to understand the factors that contribute to a successful reliability outcome because three vendors competed during the Engineering and Manufacturing Development Phase. Each vendor implemented a reliability growth program and conducted extensive testing, but only one of the vendors met the program's reliability goals. Comparing the performance of the three vendors indicates that programs should:

- Review and approve failure definition scoring criteria early to improve vendors' understanding of government priorities.
- Encourage vendors to base initial reliability predictions on operationally representative test data, to include the system, test conditions, and approved failure scoring procedures.
- Allow adequate time and funding to grow system reliability.
- Address failure modes at all severity levels; non-aborting failures may degrade the system and cause system aborts. Addressing these failures early also reduces the maintenance and logistics burden and improves system availability. Ensure there will be enough testing to support a comparative evaluation of vendor reliability outcomes for competitive programs.

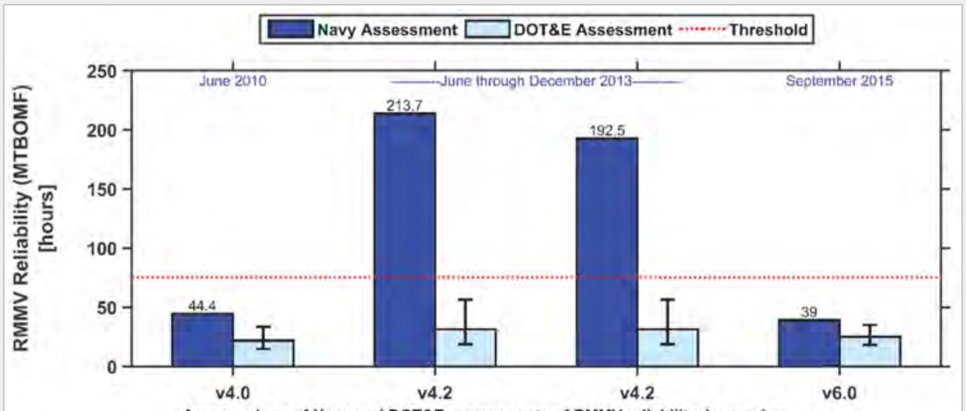
Statistically Based Reliability Analyses: Remote Multi-Mission Vehicle (RMMV)

The Remote Minehunting System (RMS) uses the RMMV, which is an unmanned, diesel-powered, semi-submersible vehicle, to tow a minehunting sonar (the AN/AQS-20 variable depth sensor).

From 2005 to 2009, the system exhibited reliability problems in nearly all periods of developmental and operational testing, twice failing to complete a planned IOT&E because of poor reliability, and ultimately experienced a Nunn-McCurdy breach. Following a Nunn-McCurdy review in 2010, USD(AT&L) directed the Navy to restructure the RMS program and fund and implement a three-phase RMMV reliability growth program.

Following combined developmental and integrated testing in 2013 (after the Navy concluded its reliability growth program), DOT&E assessed RMMV (v4.2) reliability as 31.3 hours Mean Time Between Operational Mission Failure (MTBOMF), less than half the Navy's requirement of 75 hours MTBOMF; further, DOT&E's statistical analysis of all test results indicated that reliability had not actually improved. Navy officials asserted that RMMV (v4.2) had demonstrated remarkable reliability improvements, testifying to Congress in 2013 that testing had shown reliability "substantially exceeding requirements" and in 2014 that the system "continues to test well." Throughout 2014, DOT&E detailed its analyses of RMMV v4.2 reliability in multiple memoranda to USD(AT&L) refuting the Navy's unsubstantiated claims that it had achieved reliability requirements and demonstrated readiness to restart low-rate initial production.

The Navy subsequently upgraded the RMMV v4.2 to make it compatible with the Littoral Combat Ship's (LCS) communications and launch, handling, and recovery systems and commenced ship-based testing of the so-called RMMV v6.0. This version of the system continued to experience reliability problems. In an August 2015 memorandum, DOT&E advised USD(AT&L) that the reliability of the RMS and its RMMV v6.0 was so poor that it posed a significant risk to the planned operational test of the *Independence*-variant LCS and the Increment 1 mine countermeasures (MCM) mission package and to the Navy's plan to field and sustain a viable LCS-based minehunting and mine clearance capability prior to FY20. Test data continued to refute the Navy's assertion that vehicle reliability had improved and statistical measures employed by DOT&E showed "no confidence or statistical evidence of growth in reliability over time" between RMMV v4.0, v4.2, and v6.0.



A comparison of Navy and DOT&E assessments of RMMV reliability, by version

In October 2015, the Navy delayed operational testing of the *Independence*-variant LCS equipped with the first increment of the MCM mission package pending the outcome of an independent program review, including an evaluation of potential alternatives to the RMS. The Navy chartered the review in response to an August 21, 2015, letter from Senators John McCain and Jack Reed, Chairman and Ranking Member of the Senate Committee on Armed Forces expressing concerns about the readiness to enter operational testing given the significant reliability problems observed during testing in 2015. In early 2016, following the completion of the independent review, among other actions, the Navy canceled the RMS program, halted further RMMV procurement, abandoned plans to conduct operational testing of individual MCM mission package increments, and delayed the start of LCS MCM mission package IOT&E until at least FY20. After canceling the RMS program, the Navy also announced its intention to evaluate alternatives to the RMS.

Ironically, the Navy's mine warfare resource sponsor identified a multi-function unmanned surface vessel (USV) as a "game changer" and potential RMMV replacement in 2012. In the years that followed, however, Navy officials touted RMMV reliability improvements that never materialized, reported inflated reliability estimates based on incorrect analysis, and funded additional RMMV development. The Navy did not use robust statistical analysis to assess RMMV performance objectively nor did it prioritize development of a multi-function USV capable of integrating with the RMS's towed sonar. These choices have left the Navy without a viable means of towing improved sonars when the contractor delivers initial production units next year and could delay realistic testing and fielding of the system until FY20. By accepting objective analysis of RMMV performance and committing to the USV sooner, the Navy could have avoided this unfortunate position and saved millions in RMMV development costs.

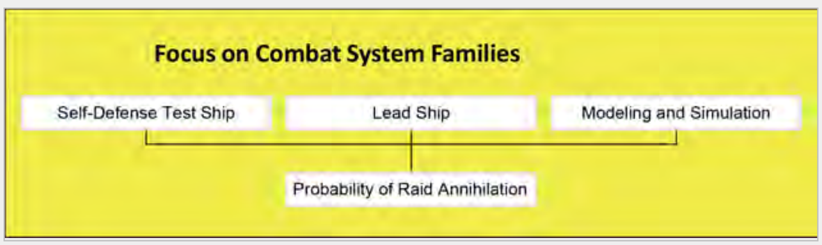
Despite DOT&E's reporting, USD(AT&L) published in its annual Developmental Test and Evaluation (DT&E) reports in March 2015 and March 2016 that RMMV v6.0 "improves vehicle performance and reliability," and that RMMV v4.2 "demonstrated sufficient reliability growth to satisfly Nunn-McCurdy requirements," citing a debunked, inflated reliability estimate of 75.3 hours MTBOMF. Such assurances from USD(AT&L) and the Navy misled their audience as to the seriousness of the problems the RMS program faced in delivering a necessary capability to the warfighter.

operational tests and evaluations, should not be accredited until a rigorous comparison of live data to the model's predictions is done. Testers should focus on the validation of the full system or environment being emulated.

Scientific Test and Analysis Techniques Center of Excellence

The Deputy Assistant Secretary of Defense for Developmental Test & Evaluation (DASD DT&E) / Director, Test Resource Management Center (TRMC) and my office continue to work collaboratively to advance the use of scientific approaches to test and evaluation. In 2011, DASD DT&E signed the Scientific Test and Analysis Techniques (STAT) Implementation Plan, which endorses these methods and created the STAT Center of Excellence (COE). The STAT COE provides program managers with the scientific and statistical expertise to plan efficient tests that ensure that programs obtain valuable information from the test program. Since 2012 when the STAT COE was formed, I have noted that programs who engage with the STAT COE early have better structured test programs that will provide valuable information. The STAT COE has provided these programs with direct access to experts in test science methods, which would otherwise have been unavailable. However, the COE's success has been hampered by unclear funding commitments. The COE must have the ability to provide independent assessments to programs (independent of the program office). Furthermore, the COE needs additional funding to aid program managers in smaller acquisition programs. Smaller programs with limited budgets do not have access to strong statistical help in their test programs and cannot afford to hire a full-time PhD-level statistician to aid their developmental test program; having access to these capabilities in the STAT COE on an as-needed basis is one means to enable these programs to plan and execute more statistically robust developmental tests. Finally, the STAT COE has also developed excellent best practices and case studies for the T&E community.

Enterprise Strategy – Testing Naval Air Defense



In 1996, the Navy defined the self-defense capability against anti-ship cruise missiles (ASCMs) that all new ship classes were required to have. This probabilistic self-defense requirement is known as the probability of raid annihilation (PRA) requirement. The PRA requirement states that a ship must defeat a raid of ASCMs, arriving within a short time window, such that no ASCMs hit the ship, and specifies with what probability of success this must be achieved. With assistance from DOT&E, the Navy developed a strategy for assessing this requirement with end-to-end testing of integrated combat systems for all new ship classes (e.g., USS *San Antonio* class, USS *America* class, USS *Zumwalt* class.). The combat systems on U.S. Navy ships are composed of many systems, which are developed by separate program offices. Before this new "enterprise" strategy, no one program office was responsible for developing the overall test program. One goal of the strategy was to consolidate all testing requirements from all sources, developmental or operational testing, for individual systems or for the overall ship, and truly create an integrated test program.

Among other things, this new enterprise strategy intended to address testing the ship-class PRA requirement and to provide for a more efficient use of test resources for conducting anti-air warfare ship self-defense testing. By addressing multiple ship class and combat system element requirements in an integrated test strategy, the Navy was able to reduce the total amount of testing required. Before using the enterprise strategy, each ship class and individual system would develop its own test program. With the enterprise strategy, a test program for the family of combat systems is developed. This allows testing to focus on the overall end-to-end mission of ship self-defense and eliminates duplicative testing. As an example, USS *San Antonio* and USS *America* are both amphibious ships that operate in similar environments against similar threats. The equipment on the *San Antonio* is a subset of the equipment on the *Americ*a.

This enterprise strategy was successfully applied to the USS *San Antonio* class. For the USS *America* class, the enterprise approach permitted testing to focus on the added components (SPS-49 radar and Evolved SeaSparrow Missile (ESSM) integration) and on incremental upgrades to the other systems. As with the USS *San Antonio* assessment, the USS *America* assessment is satisfying the ship's PRA requirements, requirements for the Block 2 Rolling Airframe Missile (RAM Blk 2), and for the Mark 2 Ship Self-Defense System (SSDS MK 2). Prior to the enterprise strategy, the Navy pursued individual test programs for each system that would have required many tests, each very similar in nature, be executed. Before adopting the enterprise approach, the Navy estimated they would spend $1.1 Billion on ship self-defense testing against cruise missiles between FY05 and FY15. The enterprise strategy reduced those costs by $240 Million and continues to provide a means to optimize the use of scarce and expensive resources.

Additionally savings related to the enterprise strategy are the results of a common modeling and simulation (M&S) paradigm for assessing the PRA requirement and some other combat system requirements. In the case of RAM Blk 2 and USS *America*, both programs needed end-to-end representations of the ship's combat system to test requirements. In this example, the M&S suite developed to assess the ship's PRA requirement is also being used to assess the missile probability of kill requirement. By using the same M&S paradigm, the live testing needed to support the verification, validation, and accreditation is also reduced. A similar approach will be applied to the next flight of the USS *America* class (i.e. LHA 8) and its combat system elements (SSDS MK 2, the Block 2 ESSM, and the Enterprise Air Surveillance Radar) and to other new ship programs (e.g., USS *Arleigh Burke* Flight III) and their combat system elements (e.g., SPY-6 Air and Missile Defense Radar).

Science of Test Research Consortium
As we work to apply more rigorous approaches to the test and evaluation of defense systems, challenges inevitably arise that demand new approaches. In collaboration with TRMC since 2011, my office continues to fund the Science of Test Research Consortium. The consortium pulls together experts in experimental design, statistical analyses, reliability, and M&S from Naval Post Graduate School, the Air Force Institute of Technology, and six additional universities. The Science of Test Research Consortium supports both the development of new techniques as well as a link between academia and the T&E community and a pipeline of graduates who could enter the T&E workforce. As advances occur in statistics, the research consortium keeps the T&E community aware of those changes. Additionally, they are working to focus research efforts on the unique challenges of operational test and evaluation that require new statistical methods. The consortium is essential for ensuring we remain well-informed of new techniques and improvements to existing techniques.

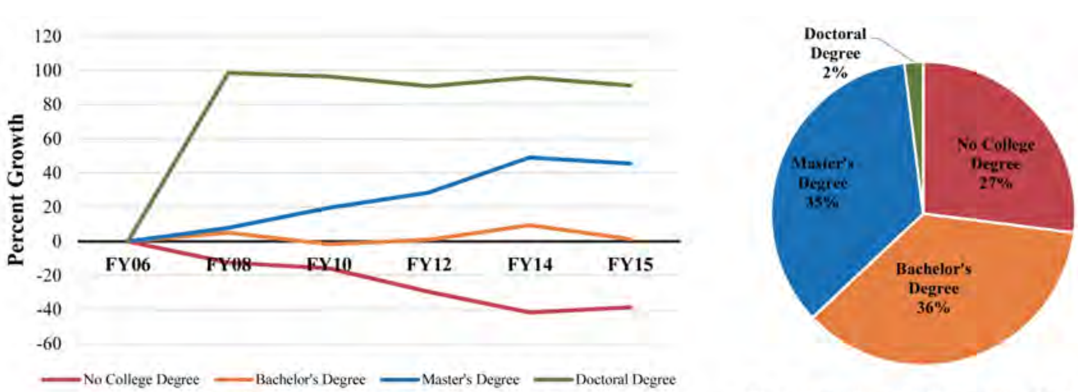
Science of Test Workshop
This past year my office, in collaboration with NASA and the Institute for Defense Analyses, supported the inaugural Test Science Workshop, which was designed to build a community around statistical approaches to test and evaluation in defense and aerospace. The workshop brought together practitioners, analysts, technical leadership, and statistical academics for a 3-day exchange of information, with opportunities to attend world-renowned short courses, share common challenges, and learn new skill sets from a variety of tutorials.

The Workshop promoted the exchange of ideas between practitioners in the T&E community with academic experts in the research consortium. Over 200 analysts from across the federal government and military Services benefited from training sessions, technical sessions, and case studies showcasing best practices. The feedback from participants was overwhelmingly positive, reinforcing that the event was much needed in the DOD and NASA analytical communities. The high response rate and enthusiastic comments indicated a clear desire to attend such events in the future.

Workforce
Rigorous and operationally realistic testing requires a skilled workforce capable of understanding the systems under test and applying scientific, statistical and analytical techniques to evaluate those systems. It is critical that personnel in the Operational Test Agencies (OTAs) have strong scientific and analytical backgrounds. In 2012, DOT&E conducted a workforce study and recommended that each OTA (1) increase the number of civilian employees with scientific, technology, engineering, and mathematics (STEM) backgrounds, (2) acquire at least one subject matter expert with an advanced degree in statistics, operations research, or systems engineering, and (3) continue to recruit military officers with operational, fleet experience.

Currently, the OTA workforce consists of roughly half civilian (51 percent) and half military (49 percent) personnel. While the overall size of the workforce has declined since 2006, the proportion of civilian personnel with advanced degrees has grown by 136 percent. The number of civilian personnel with master's and doctoral degrees increased by 45 percent and 91 percent, respectively. Currently, 2 percent of civilian personnel hold doctoral degrees, 35 percent hold master's degrees, 36 percent hold bachelor's degrees, and 27 percent do not possess a college degree. These trends are similar for each OTA and indicate that overall, OTA civilian personnel are more educated today than they were a decade ago.

Only 56 percent of civilian personnel in the OTA workforce currently hold a degree in a STEM field. However, this number includes all OTA civilian personnel, including those who do not directly engage in operational testing, such as administrators and security personnel. The proportion of civilian personnel with a degree in a STEM field increases to 72 percent when



Left: Growth in the number of civilian personnel with different degree types from FY06-FY15

Right: Proportion of civilian personnel with different degree in FY15

EDUCATION DISTRIBUTION OF CIVILIAN PERSONNEL IN THE OPERATIONAL TEST AGENCIES, FY06-FY15 these individuals are excluded, closely mirroring the proportion reported in 2012 (75 percent). Since 2012 all OTAs have acquired at least one expert with a background in statistics, operations research, or systems engineering.

The OTAs are making steady progress toward achieving the recommendations that DOT&E outlined in the 2012. The two most notable improvements since 2012 are they have all acquired expertise in statistics, operations research, or systems engineering and overall there has been an increase in the number of personnel with master's degrees.

All of the OTAs have also made significant investments in improving their capabilities for implementing rigorous statistical methods. They have updated their internal guidance and procedures to reflect DOT&E guidance. Additionally, they have all invested in training on experimental design and survey design enabling the existing workforce to better use these methods in developing and analyzing operational tests.

As military systems grow in complexity and capability, however, the need for personnel with advanced analytical capabilities, who understand scientific test design and statistics techniques, will become increasingly important and OTA hiring processes will need to continue to emphasize STEM fields.

VALUE OF INDEPENDENCE

In 1983, Congress directed OSD to create the DOT&E office, and the Director was given specific authorities in title 10 U.S. Code. The Congressional concerns that led to the establishment of this office were many, but included: poor performance of weapon systems, inaccurate reports from the Services, shortcuts in testing because of budget pressure, and a lack of realistic combat conditions and threats in testing. The unique independence of this office, free from conflicts of interest or pressure from Service senior leadership allows us to:

- Illuminate problems to DOD and Congressional Leadership to inform their decisions before production or deployment
- Tell the unvarnished truth
- Ensure operational tests are adequately designed and executed

As Director, OT&E, I do not make acquisition decisions but inform those who make them about weapon system performance under combat conditions. My staff is composed of over one-third active duty military officers from all Services in addition to civilians with advanced engineering and science degrees. Our mission is to inform acquisition officials about how weapons will work in combat, including live fire survivability and lethality, before the systems are deployed.

The independence of this office allows us to require adequate and realistic operational testing and to advocate for resources to improve our T&E capabilities. I have observed that some of the most important capabilities or tests that we have prescribed have been met with substantial resistance from the Services, sometimes requiring adjudication by the Deputy Secretary of Defense; I describe the most important of these decisions below (the T&E Resources section of this report provides details of FY16 focus areas). In light of the remarkable resistance from the Services to prioritize adequate testing and test assets in their acquisition programs, it is even more apparent that the independence of this office is critical to the success of finding problems before systems are used in combat.

Improved Test Resources for Electronic Warfare

An alarming trend I have seen during my tenure is that our threats are increasing their capabilities faster than our test infrastructure. Through the yearly budget review process, I have advocated for resources to improve test range infrastructure to support rigorous testing of modern combat systems. Most notably, in 2012, I convinced the Department to invest nearly $500 Million in the Electronic Warfare Infrastructure Improvement Program (EWIIP) to upgrade open-air test ranges, anechoic chambers, and reprogramming laboratories in order to understand performance of the F-35 Joint Strike Fighter (JSF) and other advanced air platforms against near-peer threat integrated air defense systems. The open-air test and training ranges owned and operated by both the Air Force and Navy are lacking advanced threat systems that are being used in combat by our adversaries today, are proliferating, or are undergoing significant upgrades; yet both Services strongly resisted incorporating these modern threats that we proposed until directed to do so by the Deputy Secretary.

REPROGRAMMABLE GROUND-BASED RADAR SIGNAL EMULATOR FOR USE IN OPEN-AIR TESTING OF ADVANCED AIR PLATFORMS, INCLUDING THE JOINT STRIKE FIGHTER

Moreover, an important part of the JSF mission systems is the mission data file, which contains the settings that the JSF sensors use to identify signals detected from the threat's integrated air defense systems. The United States Reprogramming Laboratory (USRL) is responsible for building the mission data file. The USRL is also a recipient of resources DOT&E argued for with the EWIIP program. Unfortunately, even though funding for upgrades was provided in 2014, preventable but now insurmountable delays configuring the USRL will delay its ability to support JSF combat capabilities until at least mid-2018.

In 2016, my office again requested funding for infrastructure to support testing and training of additional advanced air warfare systems such as the Next Generation Jammer. This funding is intended to enable the test ranges and the models and simulations (that must be validated with test data) to assess the performance of U.S. systems against the key challenges of near peer threat air defense networks of the 2020s.

Fifth-Generation Aerial Target (5GAT)

In 2006, DOT&E sponsored a study on the design of a dedicated Fifth Generation threat aircraft to adequately represent characteristics of threat aircraft being deployed by our adversaries. Since then, DOT&E and TRMC have invested over $11 Million to mature the government-owned design. The Department provided funding to complete the final design, tooling, fabrication, and flight tests. The prototyping effort will provide cost-informed alternative design and manufacturing approaches for future aerial target acquisition programs. These data can also be used to assist with future weapon system development decisions as well as T&E planning and investment, and will support future T&E analysis of alternative activities.

Self-Defense Test Ship

In 2013, the Navy sadly re-learned in the accident aboard the USS *Chancellorsville* (CG 62) where a target drone impacted the ship, that the only safe way to test the complex close-in self-defense capabilities of a ship is to mount those capabilities on a remotely controlled, unmanned self-defense test ship (SDTS). And this was not the first time such an accident occurred. In 1983, a sailor was killed onboard USS *Antrim* (FFG 20) during a test. The safety risks associated with testing short-range, self-defense systems are significant and increasing with the increasing capabilities of modern anti-ship cruise missiles. Hence, it is necessary to have test assets such as the unmanned SDTS to conduct such testing.

The SDTS has been integral in the past in testing weapons systems and ship classes. Without it, significant limitations in the Navy's ability to defend surface combatants would not be understood. Furthermore, efforts to overcome these limitations could not be tested. Unfortunately, the Navy has been reluctant to extend the same investment to developing an SDTS equipped with an Aegis Combat System, Air and Missile Defense Radar (AMDR), and Enhanced SeaSparrow Missile (ESSM) Block 2 for adequate operational testing of the DDG 51 Flight III destroyer self-defense capabilities. The current SDTS lacks the appropriate sensors and other combat system elements to test these capabilities.

In 2014, the Navy published a study that claimed an Aegis-equipped SDTS was not necessary for operational testing; however, DOT&E refuted these claims, which use flawed justifications There is no short cut. Safety considerations preclude testing against realistic threats onboard manned ships. It has been demonstrated on numerous occasions that data from less stressing manned ship testing, where targets must be fired at large crossing angles and turned away from the ship at significant ranges, cannot be extrapolated to stressing, realistic threat encounters. Modeling and simulation (M&S) cannot replace live testing because without the SDTS there are no data to ensure that the M&S accurately portray live results.

In December 2014, the Deputy Secretary of Defense commissioned a study by the Director of Cost Assessment and Program Evaluation (CAPE) to provide options to deliver an at-sea test platform adequate for self-defense operational testing of the DDG 51 Flight III, the AMDR, and the ESSM Block 2 programs. CAPE provided three affordable alternatives and the Deputy Secretary directed the Navy to procure long-lead items to begin procurement of an Aegis-equipped SDTS. The Deputy Secretary further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs, and to document that strategy in a draft Test and Evaluation Master Plan (TEMP) to be submitted by July 2016.

Despite the clear need for an Aegis-equipped SDTS and the unambiguous direction of the Deputy Secretary, the Navy has, as of the signing of this report, not yet provided an integrated test strategy for these crucial programs; and although the Navy provided funding for the long-lead AMDR components, the Navy did not program funding in the Future Years Defense Plan to complete all other activities (including procuring Aegis Combat System equipment and targets) necessary to modify the SDTS and support adequate operational testing of the DDG 51 Flight III's self-defense capabilities in FY23 as planned. In November 2016, the Deputy Secretary again directed the Navy to fully fund those activities.

Full Ship Shock Trial (FSST) for CVN 78 and DDG 1000

In hostile areas, ships commonly face the threat of underwater shocks created by non-contact detonations of torpedoes, mines, or near miss air delivered weapons. These threats do not require precise targeting or the ship to sink because the shock from a nearby miss can defeat critical mission capabilities by knocking motors and generators off-line and breaking equipment not adequately shock-mounted. Consequently, DOT&E requires shock trials for ships to test them for survivability against these widely prevalent threat types. The shock trial subjects combat-equipped ships to as operationally realistic an underwater shock load as possible while avoiding potential for crew injury and catastrophic damage. These trials are required before the first deployment of any ship class to allow for design improvements to the ship to make it more survivable in combat. Identifying these problems early in the construction of the class allows design changes to be more economically incorporated into follow-on ships. The early execution is especially critical, as each shock trial results in hundreds of findings of shock deficiencies that require correction and would not appear in M&S.

Unfortunately, the Navy, despite admitting in its technical warrants that "shock trials do have value and a return on investment," recommended in 2013 that the ship acquisition program forgo the use of shock trials as part of LFT&E or to meet Navy shock-hardening requirements. The Navy further attempted to delay shock trials on CVN 78 and DDG 1000 to later ships in the class, citing program schedule, cost, or operational availability above any scientific rationale. If the shock trial is delayed to later ships, it will occur after many years of operational deployment, exposing these ships to unnecessary risk from undiscovered and uncorrected vulnerabilities. After the Senate Armed Services Committee Chairman and Ranking Member expressed concern with this plan and urged restoration of the shock trial to the lead ship in the CVN 78 class, the Deputy Secretary directed the Navy to conduct shock trials on CVN 78 prior to first deployment, and on DDG 1000 or 1001 prior to the deployment of any ship of that class.

Warrior Injury Assessment Mannequin (WIAMan)

Commercial automotive crash test dummies were designed to assess injuries from the forces most commonly seen in civilian car accidents – sharp accelerations parallel to the ground as the car is rapidly (over milliseconds) pushed from the back, front, or side. In 2009, and repeatedly since, evaluations of combat injury data and the Department's underbody blast M&S capabilities have revealed these dummies, used only out of necessity, are wholly inadequate for predicting injuries in the direction that military vehicles and their occupants were being pushed in the field – upwards and over orders of magnitude shorter time frames resulting in completely different shock impacts. The fundamentally different nature of this impact and its effects on warfighters in vehicles exposed to an under-vehicle Improvised Explosive Device (IED), required initiating a new effort to increase DOD's previously poor understanding of the cause and nature of injuries incurred in underbody blast events, and as well as designing a military-specific anthropomorphic test device (ATD) to use in live fire test events replicating IED events.

The Department's shortcomings in this domain were a cause for concern for the Secretary of Defense in 2010. The DOT&E vulnerability assessment of the Mine Resistant Ambush Protected (MRAP) family of vehicles revealed that combat injuries, and not test data, proved that some MRAP variants provided significantly less protection than others. Upon receiving this news, Secretary Gates directed a review of the Department's underbody blast M&S capability gaps, and the top three gaps were all related to the ability to predict injuries to vehicle occupants after under-vehicle explosions. The subsequent directive to address these gaps came from senior OSD leadership, and, with initial funding from DOT&E, the Army began this project known as the Warrior Injury Assessment Manikin (WIAMan.)

Unfortunately, Army leadership continues to question the need for this capability, which threatens the successful execution of the WIAMan project, even though these threats are likely to persist into the future. The Army requirements community recognizes this threat, as demonstrated by the fact that all of their current and future ground platforms have some form of underbody protection requirement. Despite these survivability requirements for future ground combat vehicles, Army leadership continues to renew resistance to almost every aspect of the WIAMan project, from its requirements to its cost, and some claim, despite overwhelming evidence to the contrary, that the Department's current injury assessment capability is good enough. The Army Research Laboratory did not agree that the Department's current capability was adequate, and created the WIAMan Engineering Office (WEO) in 2012 to oversee the scientific research and ATD development to advance the state of the science. The WEO has led 5 years of successful research on injury assessment criteria by a consortium of university and government laboratories and the production of a prototype mannequin. Subsequently, in 2015 the Army decided that WIAMan should become an Acquisition Category II acquisition program of record similar to a combat weapon system with a formal program manager, but the Army did not provide any additional funding to establish this acquisition program office. All of the bureaucratic minutiae associated with a establishing a major program of record to build 40 articles costing less than $1 Million each has had a significantly negative impact on cost and schedule, with no demonstrable benefits. The personnel and resources required to stand up a program office whose only function is to support contracting is a questionable use of funding on a resource-constrained program. The Army should remove the WIAMan project from its acquisition system (thereby eliminating unnecessary bureaucratic overhead) and allow the WEO to develop a build-to-print prototype concept ATD; once its performance has been assessed as adequate by the WEO, the Army should solicit bids from industry to build the new ATD. A separate (unfunded) program office should not be required for this approach. As the project is currently unfunded in its entirety past FY18, DOT&E remains concerned that the Army does not intend to ultimately complete this project.

The development and fielding of the WIAMan ATD will bring the Department on par with the civilian automotive world in its ability to accurately assess injuries from traumatic events. Despite the 2011 OSD and Army approval of a well-documented project scope driven by combat injuries, Army leadership is now requiring yet another round of justification on the injuries selected for inclusion in the WIAMan ATD, and Army acquisition leadership is expressing unease with incorporating these ATDs into live fire testing up to, and including, the Advanced Multi-Purpose Vehicle. In the view of DOT&E, it is entirely appropriate for the DOD, and in particular for the Army, to accord the same high priority to testing and verifying the protection provided to soldiers by their combat vehicles that the commercial automotive industry accords to testing and verifying the protection provided to the U.S. public by their automobiles.

MYTHS ABOUT OPERATIONAL TESTING

Over the course of more than 25 years in public service, I have found it lamentable that the acquisition bureaucracy in the DOD routinely promulgates unfortunate falsehoods. I have seen and heard many inaccurate claims of what DOT&E does and does not do, and inaccurate claims about system performance that are subsequently recanted or proven wrong by this office. These falsehoods can have deleterious impacts on programs. When a program manager makes false assertions regarding the impact of operational testing on programs, there is always a risk that people in leadership positions, who have little detailed knowledge of the program, will nonetheless believe the program manager and unwisely attempt to curtail operational testing – despite the fact that operational testing requires a small fraction of the overall program's cost and schedule and all too frequently identifies significant problems with performance for the first time.

Constrained defense budgets have existed throughout my tenure, which has resulted in questions about the value of operational testing. It has also been asserted that testing is a major cause of delays in defense programs and adds uncontrolled costs. A primary purpose of operational testing, and a key value of such testing, is to identify critical problems that can be seen only when systems are examined under the stresses of realistic combat conditions, prior to the Full-Rate Production decision and fielding to combat units. This identification permits corrective action to be taken before large quantities of a system are procured and avoids expensive retrofit of system modifications. The assertion that testing causes delays misses the essential point: fixing the deficiencies causes delays, not the testing. Furthermore, taking the time to correct serious performance problems is exactly what we desire in a properly-functioning acquisition system. We are not engaged in bureaucratic game play here; testing is not a game to be won. What we do is very serious. And yes, we need to highlight the performance problems that need to be fixed so that they can be fixed.

In response to the cost of operational testing, it is relevant to consider these costs relative to the acquisition costs of the systems themselves. Numerous studies have identified that the marginal cost of operational testing is small, in general less than 1 percent of a program's overall acquisition cost. This small relative cost stands in stark contrast with the potential savings from problems identified that can be corrected before full-rate production and the likely result that the system will work when called upon in combat.

While there has been concern over the cost of operational testing throughout my tenure, I have had the opportunity to observe firsthand how necessary an independent, objective operational test is to our acquisition system. Independent, operational testing not only provides objective information for

Inaccurate claims about Operational Testing

The USD(AT&L) requests yearly assessments from program managers concerning the challenges they face; these assessments are routinely shared with the defense community without critical factual review. In a recent assessment, a program manager expressed concern regarding the negative impacts of operational testing. The program manager asserted that three releases of a major automated information system had taken an average of 12 to 18 months to complete operational testing, and that:

> … the testing community has taken almost as long to operationally test the software as the program office took to develop it in the first place. Over time, this has contributed to the cost and schedule overruns … [and] delays in delivering important capabilities to users.

The program manager went on to say that this type of operational testing issue is "systemic to defense acquisition." These are classic examples of falsehoods routinely promoted by the acquisition community to divert attention away from the real issues of problems discovered in testing that must be fixed. In this case, the operational testing revealed the system was neither operationally effective nor survivable.

The claim that the operational tests took almost as long as development is refuted by the calendar: from the beginning of this program in 2006 to the end of the Multi-Service Operational Test and Evaluation in 2015 (9 years), it took a total of five months to conduct three operational tests, less than 5 percent of the program's duration. System design and development activities required the majority of the 9-year period. The claim that operational testing delayed delivering capabilities to users is also false, not only because operational testing did not contribute to delays, but also because DOT&E is not responsible for fielding decisions. In fact, limited fielding was authorized in 2006-2007 based on an urgent operational need.

the Congress and Defense leadership, but also provides critical information to programs on improving systems so warfighters are properly equipped.

Programs clearly have an incentive to denounce testing as unfair when it reveals performance problems. Cost and schedule overruns, especially those that are the direct result of poor program management, reflect poorly on program managers and program executive officers. However, by engaging in bureaucratic games, rationalizing problems, and minimizing testing, the result is a great disservice for the people for whom we work – men and women in combat whose lives depend on the systems we field to them. There's a terrible fear that exists that a negative DOT&E report will kill a program; however, it is much more likely that performance problems reported by DOT&E lead to a greater allocation of resources and time to fix them.

Bureaucratic process is no substitute for thought and common sense. Programs often complain that DOT&E requires testing beyond threshold requirements, or even threshold KPPs. As I discussed earlier, if programs were tested solely to their KPPs, we often would not be able to evaluate whether systems can accomplish their primary missions. While we must always pay attention to requirements documents, we also have to interact with the operators. We have to pay attention to the concepts of operation, to the war plans, to the intelligence information on the latest threats, and all of those things will tell us how to do an operational test under the circumstances the system will actually be used in combat and enable us to characterize the performance of systems across their operational envelope – not just at one key parameter. For example, I have heard program managers claim there are no requirements for cybersecurity, and therefore cybersecurity should not be tested. This is an extreme example of not using common sense but hiding behind ambiguous language in DOD directives.

Exaggerated Costs of Testing

DOT&E approved a TEMP in 2012 for a program with multiple software releases planned. Separate OT&E periods were planned for selected releases depending on the capabilities introduced. Operational testing was not required for versions without meaningful mission capability enhancements. In 2014, the Service restructured this program and approved critical KPP capabilities to be delivered with one of the versions that was not originally planned to have operational testing – the Service changes were a result of development of previous releases taking much longer than predicted. Successive rounds of developmental testing revealed repeated instability and inadequate performance. After the restructure, DOT&E required the Program Office to update their TEMP to reflect the new reality. In response, the program reported to USD(AT&L) that operational test requirements would add 3 months and $9 Million additional cost and schedule. This was contrary to the Service's Operational Test Agency (OTA) estimate that the testing would take approximately 30 days and cost approximately $300,000. The delays identified by the program manger were the result of unrealistic assumptions about development and integration time periods – not because of operational testing.

Inaccurate Claims Regarding Cybersecurity Test and Evaluation

Earlier this year, the USD(AT&L) requested Program Executive Officers (PEOs) provide him assessments of the challenges they confront in their jobs; these assessments were published in the Defense Acquisition University (DAU) online magazine without critical factual review. One PEO wrote that cyber testing and the ability to achieve a survivable rating from DOT&E was nearly impossible, adding that test criteria are not well defined. The PEO went on to say that threat portrayal exceeds the capabilities of a Blue Force Team (i.e., nation-state threat going against a brigade-level formation) and focuses on insider threats of unreasonable proportions. It was especially unfortunate for this to be published widely without comment because it could inevitably undermine the efforts the operational test community has taken to find and fix the significant cybersecurity issues present in most of our acquisition programs.

While the Joint Staff is making progress formalizing cybersecurity within the survivability KPP, Secretary Carter clearly stated his common-sense requirement that all the Department's weapon systems must undergo cybersecurity assessments. And consistent with DOT&E's statutory authority, we have published specific procedures and metrics to be used to conduct cybersecurity test and evaluation for over a decade.

We have routinely seen that DOD Red Teams need to use only novice skills to successfully attack our systems. Nonetheless, the intelligence community states that virtually all major defense acquisition programs will face advanced, nation-state cyber threats. Our assessments report results for both types of threats separately.

The intelligence community also consistently describes insider threats as the primary cybersecurity threat to acquisition programs. Bradley Manning and Edward Snowden are two insiders we know; we clearly do not know about all potential insider threats. Hence it would be grossly irresponsible for OT&E to not assess insider threats, which are obviously real.

LOOKING TOWARD THE FUTURE

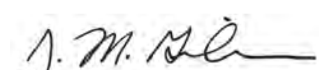
As a community we have made immense progress in the past seven years. The need for rigorous and defensible approaches to test and evaluation is not going away. As our systems become even more complex, and autonomous, continuous and integrated testing will be necessary. We will need to continue to evolve our application of state-of-the-art methodologies to confront these new challenges. We will continue to need to update range resources.

Over the past seven years, we have put the framework in place, establishing the research consortium, science of test workshop in partnership with NASA, developing guidance including the TEMP Guidebook and others. However, this office as well as the Service test organizations, need to keep moving the trajectory forward so that we continue to provide valuable information to decision makers.

The operational test community should continue to provide independent, fact-based information to senior leaders and decision makers. The Service operational test organizations, like my office, are organized to be independent from the acquisition leadership. This is so that the facts, the unvarnished truth, can be reported to senior leadership without undue influence. However, in order for real change to take place in the acquisition system and to minimize future acquisition failures, leadership must actually make itself aware of the information provided by independent assessments of systems, critically question all the information they have, and use it to make sound decisions. I have provided numerous examples in this introduction where plenty of facts about systems are available; I have provided numerous methods and techniques to obtain the facts in an effective and efficient manner depending on the program involved. But unless leaders in the department display the intellectual curiosity to create a demand signal for accurate information about their programs, and the moral courage to act faithfully on that information once it's generated, acquisition reform cannot occur. Only when leaders have the authority and confidence to say "No," when the facts reveal that a course deviation is essential to a program, change will occur. The willingness and ability to say "No" to high-risk schedules, optimistic cost estimates, and optimistic claims of technical readiness and to support those decisions within and outside the Department using cogent arguments based on the facts are essential. Leadership that does this sends a strong message by directly challenging the powerful incentives that can otherwise lead to the adoption of unachievable requirements embodied in high-risk programs that fail. While there is constant criticism of DOT&E and the Services' independent activities and pressure to constrain our independence, continued strong support by the Congress and successive Administrations of these pockets of independent and objective expertise and evaluation remains, in my view, essential.

I cannot emphasize enough the need for early, adequate, realistic, and rigorous independent operational testing on all systems to ensure what is being developed will, in fact, provide our Service men and women the capabilities they need in combat. This is especially true during this period of tight budget controls as there are not sufficient resources to correct significant problems once systems are fielded.

I submit this report, as required by law, summarizing the operational and live fire test and evaluation activities of the Department of Defense during fiscal year 2016.



J. Michael Gilmore
Director

FY16 TABLE OF CONTENTS

DOT&E Activity and Oversight
FY16 Activity Summary 1
Program Oversight 7
Problem Discovery Affecting OT&E 13

DOD Programs
Major Automated Information System (MAIS) Best Practices 23
Defense Agencies Initiative (DAI) 29
Defensive Medical Information Exchange (DMIX) 33
Defense Readiness Reporting System – Strategic (DRRS-S) 37
Department of Defense (DOD) Teleport 41
DOD Healthcare Management System Modernization (DHMSM) 43
F-35 Joint Strike Fighter 47
Global Command and Control System – Joint (GCCS-J) 109
Joint Information Environment (JIE) 113
Joint Warning and Reporting Network (JWARN) 117
Key Management Infrastructure (KMI) Increment 2 119
Next Generation Diagnostic System (NGDS) Increment 1 123
Public Key Infrastructure (PKI) Increment 2 125
Theater Medical Information Program – Joint (TMIP-J) 129

Army Programs
Army Network Modernization 133
Network Integration Evaluation (NIE) 137
Abrams M1A2 System Enhancement Program (SEP) Main Battle Tank (MBT) 141
AH-64E Apache 143
Army Integrated Air & Missile Defense (IAMD) 145
Chemical Demilitarization Program – Assembled Chemical Weapons Alternatives (CHEM DEMIL-ACWA) 147
Command Web 149
Distributed Common Ground System – Army (DCGS-A) 151
HELLFIRE Romeo and Longbow 153
Javelin Close Combat Missile System – Medium 155
Joint Light Tactical Vehicle (JLTV) Family of Vehicles (FoV) 157
Joint Tactical Networks (JTN) Joint Enterprise Network Manager (JENM) 159
Logistics Modernization Program (LMP) 163
M109A7 Family of Vehicles (FoV) Paladin Integrated Management (PIM) 167
Mid-Tier Networking Vehicular Radio (MNVR) 169
Near Real Time Identity Operations (NRTIO) 173
Patriot Advanced Capability-3 (PAC-3) 175
Soldier Protection System (SPS) 179
Spider Increment 1A M7E1 Network Command Munition 183
Warfighter Information Network – Tactical (WIN-T) 185

Navy Programs
Aegis Modernization Program 189

FY16 TABLE OF CONTENTS

AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) Program 193
Amphibious Assault Vehicle (AAV) Survivability Upgrade (AAV-SU) 197
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS) 199
AN/BLQ-10 Submarine Electronics Warfare Support System 201
AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) Sonar 203
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite 205
CH-53K – Heavy Lift Replacement Program 207
Close-in Weapon System (CIWS) – SeaRAM Variant 211
Common Aviation Command and Control System (CAC2S) 213
Consolidated Afloat Networks and Enterprise Services (CANES) 217
Cooperative Engagement Capability (CEC) 219
CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier 221
DDG 1000 *Zumwalt* Class Destroyer 227
DDG 51 Flight III Destroyer/Air and Missile Defense Radar (AMDR)/Aegis Combat System 231
Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM) 235
Distributed Common Ground System – Navy (DCGS-N) 237
E-2D Advanced Hawkeye 239
Expeditionary Transfer Dock (T-ESD) and Expeditionary Sea Base (T-ESB) 241
F/A-18E/F Super Hornet and EA-18G Growler 245
Infrared Search and Track (IRST) 249
Integrated Defensive Electronic Countermeasures (IDECM) 251
Joint Standoff Weapon (JSOW) 253
LHA 6 New Amphibious Assault Ship (formerly LHA(R)) 255
Littoral Combat Ship (LCS) 259
MH-60S Multi-Mission Combat Support Helicopter 279
Mine Resistant Ambush Protected (MRAP) Family of Vehicles (FoV) – Marine Corps 285
MK 54 Lightweight Torpedo and Its Upgrades Including High Altitude Anti-Submarine Warfare Capability 287
Mobile User Objective System (MUOS) 291
MQ-4C Triton Unmanned Aircraft System 295
MQ-8 Fire Scout 297
MV-22 Osprey 301
Next Generation Jammer (NGJ) Increment 1 303
P-8A Poseidon Multi-Mission Maritime Aircraft (MMA) 305
Remote Minehunting System (RMS) 309
Rolling Airframe Missile (RAM) Block 2 313
Ship Self-Defense for LHA(6) 315
Ship Self-Defense for LSD 41/49 319
Ship-to-Shore Connector (SSC) 321
SSN 774 *Virginia* Class Submarine 323
Standard Missile-6 (SM-6) 325
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 329
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT) 331
Tactical Tomahawk Missile and Weapon System 335
VH-92A Presidential Helicopter Replacement Program 337

FY16 TABLE OF CONTENTS

Air Force Programs
AC-130J Ghostrider 339
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) 343
Air Force Distributed Common Ground System (AF DCGS) 345
Air Operations Center – Weapon System (AOC-WS) 347
B-2 Defensive Management System Modernization (DMS-M) 351
Battle Control System – Fixed (BCS-F) 353
CV-22 Osprey 355
Defense Enterprise Accounting and Management System (DEAMS) 357
E-3 Airborne Warning and Control System (AWACS) Block 40/45 361
F-22A Advanced Tactical Fighter 365
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T) 369
Geosynchronous Space Situational Awareness Program (GSSAP) 371
Global Broadcast Service (GBS) System 373
Global Positioning System (GPS) Enterprise 377
Joint Space Operations Center (JSpOC) Mission System (JMS) 383
KC-46A 387
Massive Ordnance Penetrator (MOP) 391
Miniature Air Launched Decoy (MALD) and Miniature Air Launched Decoy – Jammer (MALD-J) 393
MQ-9 Reaper Armed Unmanned Aircraft System (UAS) 395
QF-16 Full-Scale Aerial Target (FSAT) 399
RQ-4B Global Hawk High-Altitude Long-Endurance Unmanned Aerial System (UAS) 401
Small Diameter Bomb (SDB) II 403
Space-Based Infrared System Program, High Component (SBIRS HIGH) 405

Ballistic Missile Defense Programs
Ballistic Missile Defense System (BMDS) 407
Sensors / Command and Control Architecture 411
Aegis Ballistic Missile Defense (Aegis BMD) 415
Ground-based Midcourse Defense (GMD) 421
Terminal High-Altitude Area Defense (THAAD) 423

Live Fire Test and Evaluation (LFT&E) 427

Cybersecurity 441

Test and Evaluation Resources 451

Joint Test and Evaluation (JT&E) 465

The Center for Countermeasures (CCM) 471

DOT&E Activity and Oversight

DOT&E Activity and Oversight

FY16 Activity Summary

DOT&E activity for FY16 involved oversight of 316 programs, including 30 Major Automated Information Systems. Oversight activity begins with the early acquisition milestones, continues through approval for full-rate production, and, in some instances, during full production until removed from the DOT&E oversight list.

Our review of test planning activities for FY16 included approval of 37 Test and Evaluation Master Plans (TEMPs), 89 Operational Test Plans, and 1 LFT&E Strategy (not included in a TEMP). DOT&E also rescinded approval for the AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) FOT&E Test Plan and disapproved the following two TEMPs and one Test Plan:

- T-AO(X) Fleet Replenishment Oiler TEMP
- AH-64E Version 6 Capability Apache Helicopter TEMP
- Defense Enterprise Accounting Management System (DEAMS) Verification of Fixes Test Plan

In FY16, DOT&E prepared 23 reports for Congress and SECDEF: 1 Cybersecurity report, 5 Early Fielding reports, 3 FOT&E reports, 1 Information Assurance and Interoperability report, 5 IOT&E reports, 2 LFT&E reports, 1 Operational Assessment (OA) report, 2 OT&E reports, 2 special reports, and the Ballistic Missile Defense System Annual Report. Additionally, DOT&E prepared 51 non-Congressional reports for DOD stakeholders: 10 Cybersecurity reports, 1 Early Operational Assessment report, 8 FOT&E reports, 2 Force Development Evaluation reports, 3 IOT&E reports, 1 Lead Site Verification Test report, 2 Limited User Test reports, 11 OA reports, 2 OT&E reports, 2 Operational Utility Evaluation reports, 1 Quick Reaction Assessment report, and 8 special reports. Some of these non-Congressional reports were submitted to Defense Acquisition Board (DAB) principals for consideration in DAB deliberations.

During FY16, DOT&E met with Service operational test agencies, program officials, private sector organizations, and academia; monitored test activities; and provided information to Congress, SECDEF, the Deputy Secretary of Defense, Service Secretaries, USD(AT&L), DAB principals, and the DAB committees. DOT&E evaluations are informed in large part through active on-site participation in, and observation of, tests and test-related activities. In FY16, DOT&E's experts joined test-related activities on 222 local trips within the National Capital Region and 827 temporary duty assignment trips in support of the DOT&E mission.

Security considerations preclude identifying classified programs in this report. The objective, however, is to ensure operational effectiveness and suitability do not suffer due to extraordinary security constraints imposed on those programs.

TEST AND EVALUATION MASTER PLANS / STRATEGIES APPROVED (*INCLUDES LIVE FIRE STRATEGY)

AC-130J Milestone C TEMP Version 6

Advanced Multi-Purpose (AMP) Cartridge, 120 mm: High Explosive Multi-Purpose with Tracer (HEMP-T), XM1147 TEMP*

Airborne Warning and Control System (AWACS) Block 40/45 Upgrade TEMP

Amphibious Combat Vehicle (ACV) 1.1 TEMP*

AN/BLQ-10 Submarine Electronic Warfare TEMP

B-2A Defensive Management System-Modernization (DMS-M) Milestone B TEMP

Bradley Engineering Change Proposal TEMP

CH-47F Cargo Helicopter TEMP

Defense Agencies Initiative (DAI) Increment 2 Release 3 TEMP

Defense Medical Information Exchange (DMIX) TEMP (Revised)

DOD Automated Biometric Identification System (ABIS) v1.2 TEMP

E-2D TEMP Revision D Change 1

F-22 Increment 3.2B Milestone TEMP

Global Broadcast Service TEMP Update

Ground Based Strategic Deterrent (GBSD) TEMP

Ground/Air Task Oriented Radar (G/ATOR) Milestone C TEMP

Guided Multiple Launch Rocket System (GMLRS) Alternative Warhead (AW) Rocket TEMP*

Handheld, Manpack and Small form fit (HMS) Rifleman Radio TEMP

Improved Turbine Engine Program (ITEP) TEMP

Joint Assault Bridge (JAB) TEMP*

Joint Light Tactical Vehicle (JLTV) Milestone C TEMP*

Joint Precision Aided Landing System (JPALS) Increment 1A Milestone B TEMP

Joint Surveillance Target Attack Radar System (JSTARS) Recapitalization Milestone A TEMP

Joint Warning and Reporting Network (JWARN) Increment 2 TEMP

Littoral Combat Ship (LCS) TEMP Change Pages

Logistics Modernization Program (LMP) Increment 2 Milestone C TEMP

Long Range Precision Fires (LRPF) Missile Milestone A TEMP (Pre-Decisional)*

Long Range Standoff (LRSO) Milestone A TEMP

Maneuver Control System (MCS) TEMP Annex for Command Web

Mid-tier Networking Vehicular Radio (MNVR) TEMP

MQ-4 Triton Unmanned Aircraft System (UAS) Milestone C TEMP

Multifunctional Information Distribution System (MIDS) Joint Tactical Radio System (JTRS) with Concurrent Multinetting/Concurrent Contention Receive (CMN/CCR) TEMP Annex K Revision A Change 1 Transmittal Proposal

Next Generation Jammer (NGJ) Increment 1 Milestone B TEMP

Public Key Infrastructure (PKI) Increment 2 Spiral 3 TEMP Addendum

RQ-4B Global Hawk Capstone TEMP

Teleport, Generation 3 (G3P3) TEMP Update

Third Generation Forward Looking Infrared (3GEN FLIR) B-Kit TEMP

OPERATIONAL TEST PLANS APPROVED

AC-130J Block 10 Operational Utility Evaluation Test Plan

Aegis (Ashore) Ballistic Missile Defense (ABMD) 5.0 Capability Upgrade Baseline 9B Cybersecurity IOT&E Test Plan

Aegis Weapon System (AWS) Baseline 9C Air Defense Destroyer IOT&E Plan Change 1

Airborne Warning and Control System (AWACS) Block 40/45 FOT&E Cyberspace Vulnerability Assessment Plan

AN/APR-39D(V)2 Radar Signal Detecting Set Anechoic Chamber Test Using the Joint Preflight Integration of Munitions and Electronic Systems (JPRIMES) Test Facility Test Support Plan

AN/APR-39D(V)2 Radar Signal Detecting Set Developmental Test 2 Operational Assessment Detailed Test Plan

AN/BLQ-10A Submarine Electronic Warfare Support System with Technical Insertion 10 Advanced Processor Build (APB)-11 and AN/BSD-3 Multifunction Modular Mast FOT&E Test Plan

AN/BQQ-10(V) Acoustic Rapid Commercial Off-The-Shelf Insertion (A-RCI) APB-13 Integrated Testing Data Collection Plan

AN/BYG-1(V) Combat Control System and AN/BQQ-10(V) Sonar System APB-13 Integrated Evaluation Framework

AN/BYG-1(V) Combat Control System, AN/BQQ-10 A-RCI System, and AN/BVY-1 Common Submarine Imaging System APB-13 Cybersecurity FOT&E Test Plan

AN/SQQ-89A(V)15 Surface Ship Undersea Warfare (USW) Combat System IOT&E Test Plan Change 3

Army Integrated Air and Missile Defense (AIAMD) Phases I and II Limited User Test (LUT) Test Plan

Army Integrated Air and Missile Defense (AIAMD) Phase III LUT Test Plan Change

Assault Amphibious Vehicle Survivability Upgrade, Engineering and Manufacturing Development Phase Detailed Live Fire Test Plan

Ballistic Missile Defense System (BMDS) Integrated Master Test Plan

Blue Grass Chemical Agent-Destruction Pilot Plant (BGCAPP) Test Concept Plan

Bradley A4 LFT&E Bradley Reactive Armor Tile Test Phase Combined Operational Test Agency Test Plan and Detailed Test Plan (DTP)

C-130J Block Upgrade 8.1 OA Test Plan

CH-53K OA (OT-B1) Test Plan

Combat Rescue Helicopter OA 1 Test Plan

Command Web LUT Test Plan

Common Analytical Laboratory System (CALS) Man Portable System DT/OT Plan

Common Analytical Laboratory System (CALS) User Demonstration Phase 1 Test Plan

Common Aviation Command and Control System (CAC2S) Cooperative Vulnerability Assessment Plan

Common Aviation Command and Control System (CAC2S) Increment 1 Phase 2 Operational Test Plan

Cooperative Engagement Capability (CEC) OT-D1C FOT&E Test Plan

Defense Agencies Initiative (DAI) OA Test Plan

Defense Medical Information Exchange (DMIX) Release 3 Operational Test Plan

Defense Medical Information Exchange/Joint Legacy Viewer (DMIX/JLV) Release 2 Verification of Corrected Deficiencies Event Test Plan

Department of the Navy Large Aircraft Infrared Countermeasure (DoN LAIRCM) V-22 Urgent Universal Need Statement Developmental Test Data Collection Plan

Department of the Navy Large Aircraft Infrared Countermeasure with Advanced Threat Warning (DoN LAIRCM ATW) AH-64, CH-47, and H-60 Integration Test Plan

Department of the Navy Large Aircraft Infrared Countermeasure with Advanced Threat Warning (DoN LAIRCM ATW) KC-130J Data Collection Plan

E-2D Advanced Hawkeye FOT&E Test Plan

E-2D OT-D2 Cybersecurity Test Plan

Expeditionary Mobile Base (ESB) IOT&E Test Plan

F/A-18E/F Infrared Search and Track System (IRST) Block I OA II Test Plan

F-35 Joint Strike Fighter (JSF) Air Vehicle Cybersecurity Cooperative Vulnerability and Penetration Assessment Plan

F-35 Joint Strike Fighter (JSF) Cybersecurity Operational Test Plan

Global Broadcast System FOT&E-1 Test Plan

Global Command and Control System – Joint (GCCS-J) Version 4.3 Cybersecurity Test Plan

Global Lightning 16 Assessment Plan

Global Thunder 16 Assessment Plan

Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK) Operational Test Agency Test Plan and Detailed Test Plan Revision

Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK) Operational Test Agency Test Plan

Integrated Master Test Plan (IMTP) v17.0

Jackal Stone (U.S. European Command) Assessment Plan

Jackal Stone (U.S. Special Operations Command) Assessment Plan

Joint Warning and Reporting Network (JWARN) IOT&E Test Plan

LHA(R) Amphibious Assault Ship Replacement (LHA(R) FLT 0) Cybersecurity IOT&E / Ship Self Defense System (SSDS) MK 2 MOD 4 Cybersecurity FOT&E Test Plan

LHA(R) Amphibious Assault Ship Replacement (LHA(R) FLT 0) IOT&E Test Plan

Littoral Combat Ship (LCS) 4 Total Ship Survivability Trial Plan

Littoral Combat Ship (LCS) 4 with Surface Warfare (SUW) Mission Package Increment 2 Cybersecurity IOT&E Test Plan

Littoral Combat Ship (LCS) 5 Shock Trial Plan

Littoral Combat Ship (LCS) 6 Full Ship Survivability Trial Plan

Littoral Combat Ship (LCS) *Independence*-Variant ET-11B Phase 1 Air Warfare Data Collection Plan

M109 Family of Vehicles, M109A7 Self-Propelled Howitzer (SPH) and M992A3 Carrier, Ammunition, Tracked (CAT) Full-Up System-Level Test Operational Test Agency Test Plan and Detailed Test Plan

M109 Family of Vehicles IOT&E Test Plan

M1A2 Abrams System Enhancement Package Version 3 (SEPv3) Engineering Change Proposal 1a Turret Half-Bustle Ammunition Vulnerability Test Phase I LFT&E Test Plan

Marine Corps Forces Central Command (MARCENT) Forward Site Assessment

MK 48 MOD 7 Common Broadband Advanced Sonar System (CBASS) Torpedo with APB-5 Software Integrated Evaluation Framework Revision 1 (Change One)

MK 54 MOD 1 Lightweight Torpedo (LWT) Increment 1 LFT&E Test Plan

Mobile Landing Platform (MLP) Total Ship Survivability Trial Plan

Mobile User Objective System (MUOS) MOT&E Test Plan

MQ-8C System OA Test Plan

MQ-9 FOT&E Test Plan

Navy Multiband Terminal (NMT) FOT&E Test Plan

Next Generation Diagnostic System (NGDS) Increment 1 OA Test Plan

Offensive Anti-Surface Warfare (OASuW) Increment 1 Long Range Anti-Ship Missile (LRASM) Master Test Strategy

Pacific Sentry 16 Assessment Plan

PANAMAX 2016 Final Assessment Plan

Patriot Post-Deployment Build-8 (PFB-8) IOT&E Test Plan

Pueblo Chemical Agent-Destruction Pilot Plant (PCAPP) Test Evaluation Plan

Ship Self-Defense System (SSDS) MK 2 FOT&E Test Plan

Small Arms Protective Insert (SAPI) Foreign Military Sales Lot Acceptance Test Detailed Test Plan

Small Diameter Bomb II (SDB-II) LFT&E Hybrid Testing Plan

Small Diameter Bomb, Increment II (SDB II) Live Fire Flight Tests (LF 07 – LF 10) LFT&E Test Plan

Soldier Protection System (SPS) Torso and Extremity Protection (TEP) Expanded Developmental Test Detailed Test Plan

Soldier Protection System (SPS) Vital Torso Protection (VTP) Enhanced Small Arms Protective Insert (ESAPI) First Article Test Detailed Test Plan

Space-Based Infrared System (SBIRS) Block 10 Operational Utility Evaluation Test Plan

Spider M7E1 Increment 1A (SI1A), LUT Test Plan

SSN 774 *Virginia* Class Block III Submarines Cybersecurity Test Plan

Stryker Family of Vehicles Engineering Change Proposal Operational Test Agency Test Plan and Detailed Test Plan

Stryker Family of Vehicles World Wide Fielding Detailed Live Fire Test Plan Deviation

Stryker Family of Vehicles World Wide Fielding Operational Test Agency Test Plan and Detailed Test Plan

Surface Electronic Warfare Improvement Program (SEWIP) Block 2 IOT&E Test Plan Change Transmittal 3

Surface Electronic Warfare Improvement Program (SEWIP) Block 2 TECHEVAL Phase B Test Plan

Theater Medical Information Program – Joint (TMIP-J) Increment 2 Release 3 MOT&E Test Plan – Navy Annex

U.S. Marine Corps Large Scale Exercise Assessment Plan

Valiant Shield 16 Assessment Plan

LIVE FIRE TEST AND EVALUATION STRATEGY APPROVED

Soldier Protection System (SPS) Live Fire Strategy

TABLE 1. FY16 REPORTS TO CONGRESS	
PROGRAM	DATE
Cybersecurity Report	
Department of Defense (DOD) Cybersecurity During Fiscal Year 2014 and Early Fiscal Year 2015	November 2015
Early Fielding Reports	
Aegis Baseline 9C Cruiser	November 2015
SLQ-32(V)6 Surface Electronic Warfare Improvement Program (SEWIP) Block 2 Upgrade	December 2015
Rolling Airframe Missile (RAM) Block 2	March 2016
Littoral Combat Ship (LCS) 2 with Mine Countermeasures (MCM) Mission Package (MP) Increment 2	June 2016
Massive Ordnance Penetrator (MOP) Enhanced Threat Response (ETR) Phase 3	September 2016
Follow-on Operational Test and Evaluation Reports	
Advanced Processing Build 2011 (APB-11) Acoustic Rapid Commercial Off-the-Shelf (A-RCI) Insertion	November 2015
Multi-static Active Coherent (MAC) System in P-8A Poseidon	December 2015
Distributed Common Ground System – Army (DCGS-A) Increment 1 Release 2 with classified cyber annex	January 2016
Information Assurance and Interoperability Report	
Defensive Cyberspace Operations (DCO) Report on Observations from FY13-15	July 2016
Initial Operational Test and Evaluation Reports	
AN/TPQ-53 (Q-53) Radar (with classified annex)	October 2015
Surveillance Towed-Array Sensor System (SURTASS) with the Compact Low-Frequency Active (CLFA) System	January 2016
Precision Guidance Kit (PGK)	March 2016
Common Aviation Command and Control System (CAC2S), Increment 1, Phase 2	August 2016
Surface Electronic Warfare Improvement Program (SEWIP) Block 2	September 2016
Live Fire Test and Evaluation Reports	
Multiple Launch Rocket (MLRS) M270A1 Launcher Improved Armored Cab (IAC)	June 2016
Soldier Protection System (SPS) Torso and Extremities Protection (TEP)	September 2016
Operational Assessment Report	
Ballistic Missile Defense Systems (BMDS) European Phased Adaptive Approach (EPAA) Phase 2 Assessment Report	March 2016
Operational Test and Evaluation Reports	
M829A4 120 mm Armor-Piercing, Fin-Stabilized, Discarding Sabot - Tracer (APFSDS-T)	December 2015
Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation 2 Report with Classified Annex	June 2016
Special Reports	
DOT&E classified and redacted/unclassified inputs for the report required by Section 123 the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) (Update from FY14 and FY15 Inputs)	January 2016
Market Survey of Active Protection Systems (APS) for Ground Combat and Tactical Wheeled Vehicles	June 2016
Ballistic Missile Defense System Report	
FY15 Assessment of the Ballistic Missile Defense System (includes unclassified Executive Summary)	April 2016

TABLE 2. FY16 NON-CONGRESSIONAL REPORTS	
PROGRAM	DATE
Cybersecurity Reports	
Global Lightning 2014 (GL14) and GL15 Cybersecurity Assessment	October 2015
Austere Challenge 15 Cybersecurity Assessment	November 2015
Turbo Challenge 15 Cybersecurity Assessment	November 2015
Pacific Sentry 2015-3 Cybersecurity Assessment	February 2016
Cybersecurity Assessment of Special Operations Command Pacific (SOCPAC) Tempest Wind 2015 Exercise	March 2016
Marine Forces Central Command (MARCENT) Forward (FWD) Cybersecurity Assessment	May 2016
Global Thunder 16 Cybersecurity Assessment	May 2016
USS *Harry S. Truman* Carrier Strike Group (HSTCSG) Composite Unit Training Exercise 2015	June 2016
Global Command and Control System – Joint (GCCS-J) Operational Cybersecurity Testing	August 2016
Cybersecurity Assessment of U.S. Africa Command (USAFRICOM) During Epic Guardian Exercise	September 2016
Early Operational Assessment Report	
Next Generation Jammer (NGJ)	February 2016
Follow-on Operational Test and Evaluation Reports	
Integrated Personnel and Pay System – Army (IPPS-A) Increment 1 Cybersecurity Evaluation	October 2015
M30A1 Guided Multiple Launch Rocket System Alternative Warhead (GMLRS-AW)	November 2015
Joint Warning and Reporting Network (JWARN) Increment 1 FOT&E-3 with classified annex	December 2015
Gray Eagle One System Remote Video Terminal (OSRVT) with classified annex	January 2016
Distributed Common Ground System – Navy (DCGS-N) Increment 1 Block 2 with classified Annex	May 2016
E-2D Advanced Hawkeye (AHE)	May 2016
OT-IIIC of Upgrades to Marine Corps AH-1Z Attack and UH-1Y Utility Helicopters (H-1 Upgrades)	May 2016
Department of the Navy Large Aircraft Infrared Countermeasures (DoN LAIRCM) Advanced Threat Warning (ATW) System	June 2016
Force Development Evaluation Reports	
Assessment of the Air Operations Center – Weapon System (AOC-WS) 10.1 Recurring Event 13	October 2015
Air Force Distributed Common Ground System (AF DCGS) Geospatial Intelligence (GEOINT) Baseline 4.1	November 2015
Initial Operational Test and Evaluation Reports	
Logistics Modernization Program (LMP) Increment 2 Wave 3 with classified Annex	April 2016
Defense Readiness Reporting System-Strategic (DRRS-S) with classified Annex	April 2016
RQ-4B Global Hawk Block 40	August 2016
Lead Site Verification Test Report	
Global Combat Support System – Army (GCSS-A)	November 2015
Limited User Test Reports	
Key Management Infrastructure (KMI) Spiral 2 Spin 1 Limited User Test Retest	October 2015
Mid-Tier Networking Radio (MNVR)	November 2015

TABLE 2. FY16 NON-CONGRESSIONAL REPORTS (CONTINUED)	
PROGRAM	**DATE**
Operational Assessment Reports	
Defense Medical Information Exchange (DMIX) Release 2 Classified Appendix (Cybersecurity Assessment)	November 2015
MaxxPro Long Wheel Base Ambulance (LWB) with classified Live Fire Report	December 2015
DOD Teleport Generation 3, Phase 3 with classified Annex	December 2015
Defense Agency Initiative (DAI) Operational Assessment	February 2016
MQ-4C Triton Operational Assessment	May 2016
MQ-8C Fire Scout Operational Assessment	June 2016
Mid-Tier Network and Mid-tier Networking Vehicular Radio (MNVR) Milestone C Operational Assessment	July 2016
F-22A Increment 3.2B Operational Assessment and Readiness for Milestone C Findings and Observations	July 2016
Defense Agency Initiative (DAI) Operational Assessment Report with classified Annex	August 2016
KC-46A Operational Assessment #2 with classified Annex	August 2016
Warfighter Information Network - Tactical (WIN-T) Increment 3 Operational Assessment with classified annex	September 2016
Operational Test and Evaluation Reports	
Theater Medical Information Program – Joint (TMIP-J) Multi-Service Operational Test and Evaluation (MOT&E) Report with classified Annex	March 2016
Defense Medical Information Exchange (DMIX) Release 3 (R3) Multi-Service Operational Test and Evaluation (MOT&E)	July 2016
Operational Utility Evaluation Reports	
Operational Utility Evaluation of Block 10 AC-130J Gunship	June 2016
Air Force Distributed Common Ground System (AF DCGS) System Release 3.0 (SR 3.0)	July 2016
Quick Reaction Assessment Report	
MQ-8B Fire Scout Radar	March 2016
Special Reports	
Littoral Combat Ship (LCS) and Mine Countermeasures (MCM) Mission Package Increment 1 Performance (Interim Assessment)	November 2015
Defense Medical Information Exchange (DMIX) Release 2 Verification of Corrected Deficiencies (VCD) Report	February 2016
Defense Enterprise Accounting Management System (DEAMS) Verification of Fixes (VoF) Test	February 2016
DOD Enterprise Cyber Range Environment (DECRE) Report	March 2016
P-8A Multi-mission Maritime Aircraft Data Storage Architecture Upgrade (DSAU) and Verification of Correction of Deficiencies (VCD)	May 2016
5.56x45 mm Cartridge Ammunition Study	August 2016
RQ-21A Blackjack Small Tactical Unmanned Aircraft System (STUAS) Initial Operational Test and Evaluation (IOT&E) Report Addendum	August 2016
Approval of Military Combat Helmet Test Protocol Standard for Ballistic Testing for the Enhanced Combat Helmet (ECH) (Updated)	September 2016

Program Oversight

DOT&E is responsible for approving the adequacy of plans for operational test and evaluation and for reporting the operational test results for all Major Defense Acquisition Programs (MDAPs) to Congress, SECDEF, the Service Secretaries, and USD(AT&L). Section 2430 of title 10, U.S. Code (10 USC 2430) defines MDAPs as those DOD acquisition programs that are not highly classified and that either meet high-dollar thresholds for research, development, test, and evaluation expenditure or have been designated as MDAPs by the SECDEF. These programs are included in Selected Acquisition Reports (SARs) submitted by USD(AT&L) to Congress. Additionally, 10 USC 139(a)(2)(B) stipulates that DOT&E may designate any other programs as MDAPs for the purpose of oversight, review, and reporting. Including such "non-major" programs, DOT&E was responsible for oversight of a total of 316 acquisition programs during FY16.

Non-major programs are selected for DOT&E oversight after careful consideration of the relative importance of the individual program. One or more of the following essential elements are considered when determining non-SAR systems for oversight:

- Congress or OSD agencies have expressed a high level of interest in the program.
- Congress has directed that DOT&E assess or report on the program as a condition for progress or production.
- The program requires joint or multi-Service testing (10 USC 139(b)(4) requires DOT&E to "coordinate operational testing conducted jointly by more than one military department or defense agency").
- The program exceeds or has the potential to exceed the dollar threshold definition of a major program according to DOD Directive 5000.01, but does not appear on the current SAR list (e.g., highly-classified systems).
- The program has a close relationship to or is a key component of a major program.
- The program is an existing system undergoing major modification.
- The program was previously a SAR program and operational testing is not yet complete.

DOT&E is also responsible for the oversight of LFT&E programs in accordance with 10 USC 139. DOD regulation uses the term "covered system" to include all categories of systems or programs identified in 10 USC 2366 as requiring LFT&E. Systems or programs that do not have acquisition points referenced in 10 USC 2366, but otherwise meet the statutory criteria, are considered covered systems for the purpose of DOT&E oversight.

DOT&E has determined that a covered system, for the purpose of oversight for LFT&E, meets one or more of the following criteria:

- A major system, within the meaning of that term in 10 USC 2302(5), that is:
  - User-occupied and designed to provide some degree of protection to the system or its occupants in combat
  - A conventional munitions program or missile program
- A conventional munitions program for which more than 1,000,000 rounds are planned to be acquired.
- A modification to a covered system that is likely to affect significantly the survivability or lethality of such a system.

DOT&E was responsible for the oversight of 132 LFT&E acquisition programs during FY16.

Programs Under DOT&E Oversight
Fiscal Year 2016
(As taken from the September 2016 DOT&E Oversight List)

DOD PROGRAMS

AC-130J

BMDS - Ballistic Missile Defense System Program

CHEM DEMIL-ACWA - Chemical Demilitarization Program - Assembled Chemical Weapons Alternatives

CHEM DEMIL-CMA - Chemical Demilitarization (Chem Demil) - Chemical Materals Agency (Army Executing Agent)

Common Analytical Laboratory System

Defense Agency Initiative (DAI)

Defense Enterprise Accounting and Management System - Increment 1 (DEAMS - Inc. 1)

Defense Medical Information Exchange (DMIX)

Defense Security Assistance Management System (DSAMS) - Block 3

DoD Healthcare Management System Modernization (DHMSM)

EDS - Explosive Destruction System

Enterprise SATCOM Gateway Modem

EProcurement

DOD PROGRAMS (continued)

Global Command & Control System - Joint (GCCS-J)
Joint Aerial Layer Network
Joint Biological Tactical Detection System
Joint Information Environment
Joint Light Tactical Vehicle (JLTV)
Joint Operational Medicine Information Systems
Joint Regional Security Stack (JRSS)
Joint Warning and Reporting Network (JWARN)
Key Management Infrastructure (KMI) Increment 2
Mid-Tier Networking Vehicle Radio
milCloud
Modernized Intelligence Database (MIDB)
Modernized Intelligence Database (MIDB)
Multi-Functional Information Distribution System (includes integration into USAF & USN aircraft)
Next Generation Chemical Detector
Next Generation Diagnostic System Increment 1 (NGDS Inc 1)
Public Key Infrastructure (PKI) Increment 2
SOCOM Dry Combat Submersible Medium (DCSM)
Teleport, Generation III
Theater Medical Information Program - Joint (TMIP-J) Block 2

ARMY PROGRAMS

3rd Generation Improved Forward Looking Infrared (3rd Gen FLIR)
Abrams Active Protection Systems (APS)
ABRAMS TANK MODERNIZATION - Abrams Tank Modernization (M1E3)
Abrams Tank Upgrade (M1A1 SA / M1A2 SEP)
Advanced Field Artillery Tactical Data System (AFATDS) Version 7
Advanced Multi-Purpose (AMP) 120 mm Tank Round
AH-64E Apache Remanufacture/New Build
Airborne and Maritime/Fixed Site Joint Tactical Radio System (AMF JTRS) Small Airborne Networking Radio (SANR)
AN/PRC-117G Radio
AN/TPQ-53 Radar System (Q-53)
Armored Multipurpose Vehicle (AMPV)
Armored Truck - Heavy Dump Truck (HDT)
Armored Truck - Heavy Equipment Transporter (HET)
Armored Truck - Heavy Expanded Mobility Tactical Truck (HEMTT)
Armored Truck - M915A5 Line Hauler
Armored Truck - M939 General Purpose Truck
Armored Truck - Palletized Loading System (PLS)
Army Integrated Air & Missile Defense (AIAMD)
Army Tactical Missile System - Service Life Extension Program (ATACMS-SLEP)
Army Vertical Unmanned Aircraft System
Assured Precision, Navigation & Timing (Assured PNT)
Biometrics Enabling Capability (BEC) Increment 1
Biometrics Enabling Capability Increment 0
Black HAWK (UH-60M) - Utility Helicopter Program
Bradley Active Protection Systems (APS)
Bradley Engineering Change Proposal (ECP) and Modernization
Brownout Rotorcraft Enhancement System (BORES)
C-17 Increase Gross Weight (IGW) and reduced Formation Spacing Requirements (FSR) with T-11 parachute
Cannon Delivered Area Effects Munitions (C-DAEM) Family of Munitions
CH-47F - Cargo Helicopter
Chinook H-47 Block II
Command Post Computing Environment (CPCE)
Common Infrared Countermeasures (CIRCM)
Common Remotely Operated Weapons System III
Data Center / Cloud / Generating Force Computing Environment (DC/C/GFCE)
Department of Defense Automated Biometric Information System
Distributed Common Ground System - Army (DCGS-A)
EXCALIBUR - Family of Precision, 155 mm Projectiles
Family of Small Unmanned Aircraft Systems
FBCB2 - Force XXI Battle Command Brigade and Below Program
FBCB2 - Joint Capability Release (FBCB2 - JCR)
Fixed-Wing Utility Aircraft
FMTV - Family of Medium Tactical Vehicles
Future Vertical Lift Capability Set 3 (FVL CS 3)
Gator Landmine Replacement Program (GLRP)
General Fund Enterprise Business System (GFEBS)
Global Combat Support System - Army (GCSS-A)
Guided Multiple Launch Rocket System - Unitary (GMLRS Unitary)
Guided Multiple Launch Rocket System Alternate Warhead (GMLRS AW)
HELLFIRE Romeo
High Explosive Guided Mortar (HEGM)
High Mobility Multipurpose Wheeled Vehicle (HMMWV)
HIMARS - High Mobility Artillery Rocket System
Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
Improved Turbine Engine Program
Indirect Fire Protection Capability Increment 2 - Intercept

ARMY PROGRAMS (continued)

Integrated Personnel and Pay System - Army (Army IPPS) Increment 1
Integrated Personnel and Pay System - Army (IPPS-A) Increment 2
Interceptor Body Armor
Javelin Antitank Missile System - Medium
Joint Air-to-Ground Missile
Joint Assault Bridge
Joint Battle Command Platform (JBC-P)
Joint Tactical Networks (JTN)
Logistics Modernization Program (LMP)
Long Range Precision Fires (LRPF)
M270A1 Multiple Launch Rocket System (MLRS)
M829A4
M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System (Hercules)
Mine Resistant Ambush Protected Vehicle Systems - including SOCOM vehicles
Mobile / Handheld Computing Environment (M/HCE)
Mobile Protected Firepower Increment 1 (MPF Inc 1)
Modernized Expanded Capacity Vehicle (MECV) - Survivability Project
Mounted Computing Environment (MCE)
MQ-1C Unmanned Aircraft System Gray Eagle
Near Real Time Identity Operations
Nett Warrior
One System Remote Video Terminal
Paladin/FASSV Integrated Management (PIM)
PATRIOT PAC-3 - Patriot Advanced Capability 3 (Missile only)
Real Time / Safety Critical / Embedded Computing Environment (RT/SC/ECE)
RQ-7B SHADOW - Tactical Unmanned Aircraft System
Sensor Computing Environment (SCE)
Soldier Protection System
Spider XM7 Network Command Munition
Stryker Active Protection Systems (APS)
STRYKER ECP - STRYKER Engineering Change Proposal
Stryker M1126 Infantry Carrier Vehicle including Double V-Hull variant
Stryker M1127 Reconnaissance Vehicle
Stryker M1128 Mobile Gun System
Stryker M1129 Mortar Carrier including the Double V-Hull variant
Stryker M1130 Commander's Vehicle including the Double V-Hull Variant
Stryker M1131 Fire Support Vehicle Including the Double V-Hull Variant
Stryker M1132 Engineer Squad Vehicle Including the Double V-Hull Variant
Stryker M1133 Medical Evacuation Vehicle Including the Double V-Hull Variant
Stryker M1134 ATGM Vehicle Including the Double V-Hull Variant
Stryker M1135 NBC Reconnaissance Vehicle (NBCRV)
Tactical Radio System Manpack
Tactical Radio System Rifleman Radio
UH-60V Black HAWK
UH-72A Lakota Light Utility Helicopter
WIN-T INCREMENT 1 - Warfighter Information Network - Tactical Increment 1
WIN-T INCREMENT 2 - Warfighter Information Network - Tactical Increment 2
WIN-T INCREMENT 3 - Warfighter Information Network - Tactical Increment 3
XM1156 Precision Guidance Kit (PGK)
XM1158 7.72 mm Cartridge
XM17 Modular Handgun System (XM17)
XM25, Counter Defilade Target Engagement (CDTE) System

NAVY PROGRAMS

Acoustic Rapid COTS Insertion for SONAR
Advanced Airborne Sensor
Advanced Arresting Gear
Advanced Extremely High Frequency Navy Multiband Terminal Satellite Program (NMT)
Advanced Off-board Electronic Warfare Program
AEGIS Modernization (Baseline Upgrades)
AGM-88E Advanced Anti-Radiation Guided Missile
AH-1Z
AIM-9X - Air-to-Air Missile Upgrade Block II
Air and Missile Defense Radar (AMDR)
Air Warfare Ship Self Defense Enterprise
Airborne Laser Mine Detection System (AN/AES-1) (ALMDS)
Airborne Mine Neutralization System (AN/ASQ-235) (AMNS)
Airborne Resupply/Logistics for Seabasing
Amphibious Assault Vehicle Upgrade
Amphibious Combat Vehicle Phase 1 Increment 1 (ACV 1.1)
AN/APR-39 Radar Warning Receiver
AN/AQS-20 Minehunting Sonar (all variants)
AN/BLQ-10 Submarine Electronics Support Measures
AN/SQQ-89A(V) Integrated USW Combat Systems Suite
Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System Block I

NAVY PROGRAMS (continued)

Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System Block II

Barracuda Mine Neutralization System

CANES - Consolidated Afloat Networks and Enterprise Services

CH-53K - Heavy Lift Replacement Program

Close-In Weapon System (CIWS) including SEARAM

CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)

COBRA JUDY REPLACEMENT - Ship-based radar system

Common Aviation Command and Control System (CAC2S)

Cooperative Engagement Capability (CEC)

Countermeasure Anti-Torpedo

CVN-78 - *GERALD R. FORD* CLASS Nuclear Aircraft Carrier

DDG 1000 - *ZUMWALT* CLASS Destroyer - includes all supporting PARMs and the lethality of the LRLAP and 30mm ammunition

DDG 51 - *ARLEIGH BURKE* CLASS Guided Missile Destroyer - includes all supporting PARMs

DDG 51 Flight III - *ARLEIGH BURKE* CLASS Guided Missile Destroyer - includes all supporting PARMs

Dept of Navy Large Aircraft Infrared Countermeasures Program

Distributed Common Ground System - Navy (DCGS-N)

E-2D Advanced Hawkeye

EA-18G - Airborne Electronic Attack

Electro-Magnetic Aircraft Launching System

Electronic Procurement System

Enhanced Combat Helmet

Enterprise Air Surveillance Radar (EASR) (replacement for SPS-48 and SPS-49 air surveillance radars)

Evolved Sea Sparrow Missile (ESSM)

Evolved Sea Sparrow Missile Block 2

Expeditionary Transfer Dock (formerly Mobile Landing Platform (MLP) Core Capability Set (CCS) Variant) and Expeditionary Mobile Base (formerly MLP Afloat Forward Staging Base (AFSB) Variant)

F/A-18E/F - SUPER HORNET Naval Strike Fighter

Future Pay and Personnel Management Solution (FPPS)

Ground/Air Task Oriented Radar (G/ATOR)

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Infrared Search and Track System

Integrated Defensive Electronic Countermeasures

Joint and Allied Threat Awareness System

Joint Precision Approach and Landing System

Joint Stand-Off Weapon C-1 variant (JSOW C-1)

KC-130J

Landing Ship Dock Replacement (LX(R))

Large Displacement Unmanned Undersea Vehicle

LCS Surface Warfare Mission Package Increment 3--Interim Surface to Surface Missile including Longbow Hellfire Missile (or other candidate missiles and their warheads)

LHA 6 - *AMERICA* CLASS - Amphibious Assault Ship - includes all supporting PARMs

LHA 8 Amphibious Assault Ship (*America* Class with well deck)

Light Armored Vehicle

Light Weight Tow Torpedo Countermeasure (part of LCS ASW Mission Module)

Littoral Combat Ship (LCS) - includes all supporting PARMs, and 57mm lethality

Littoral Combat Ship Frigate modifications

Littoral Combat Ship Mission Modules including 30mm

Littoral Combat Ship Surface-to-Surface Missile (follow on to the interim SSM)

Littoral Combat Ship Veriable Depth Sonar (LCS VDS)

Logistics Vehicle System Replacement

LPD 17 - *SAN ANTONIO* CLASS - Amphibious Transport Dock Ship - includes all supporting PARMs and 30mm lethality

LSD 41/49 Replacement

Maritime Tactical Command and Control

MH-60R Multi-Mission Helicopter Upgrade

MH-60S Multi-Mission Combat Support Helicopter

Mk 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)

MK-48 CBASS Torpedo including all upgrades

Mobile User Objective System (MUOS)

MQ-4C Triton

MQ-8 Fire Scout Unmanned Aircraft System

Multi-static Active Coherent (MAC) System CNO project 1758

MV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey

Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air

Navy Enterprise Resource Planning (ERP)

Next Generation Jammer

Next Generation Land Attack Weapon

Offensive Anti-Surface Warfare Increment 1

Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)

OHIO Replacement Program (Sea-based Strategic Deterrence) - including all supporting PARMs

P-8A Poseidon Program

Remote Minehunting System (RMS)

Replacement Oiler

Rolling Airframe Missile (RAM) including RAM Block 1A Helicopter Aircraft Surface (HAS) and RAM Block 2 Programs

RQ-21A Unmanned Aircraft System (UAS)

Ship Self Defense System (SSDS)

NAVY PROGRAMS (continued)

Ship to Shore Connector

Small Surface Combatant (also called the Frigate modification to the Littoral Combat Ship variants) including the Anti-Submarine and Surface Warfare component systems

SSN 774 *VIRGINIA* Class Submarine

SSN 784 *VIRGINIA* Class Block III Submarine

Standard Missile 2 (SM-2) including all mods

Standard Missile-6 (SM-6)

Submarine Torpedo Defense System (Sub TDS) including countermeasures and Next Generation Countermeasure System (NGCM)

Surface Electronic Warfare Improvement Program (SEWIP) Block 2

Surface Electronic Warfare Improvement Program (SEWIP) Block 3

Surface Mine Countermeasures Unmanned Undersea Vehicle (also called Knifefish UUV) (SMCM UUV)

Surveillance Towed Array Sonar System/Low Frequency Active (SURTASS/LFA) including Compact LFA (CLFA)

Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)

Torpedo Warning System (Previously included with Surface Ship Torpedo Defense System) including all sensors and decision tools

TRIDENT II MISSILE - Sea Launched Ballistic Missile

UH-1Y

Unmanned Carrier Launched Airborne Surveillance and Strike System

Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)

USMC MRAP-Cougar

VH-92A Presidential Helicopter

AIR FORCE PROGRAMS

20mm PGU-28/B Replacement Combat Round

Advanced Pilot Trainer

AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program

AFNet Modernization capabilities (Bitlocker, Data at Rest (DaR), Situational Awareness Modernization (SAMP))

AIM-120 Advanced Medium-Range Air-to-Air Missile

Air Force Distributed Common Ground System (AF-DCGS)

Air Force Integrated Personnel and Pay System (AF-IPPS)

Air Force Mission Planning Systems Increment 5

Air Force Organic Depot Maintenance, Repair and Overhaul Initiative (MROi)

Air Operations Center - Weapon System (AOC-WS) 10.1

Air Operations Center - Weapon System (AOC-WS) 10.2

Airborne Signals Intelligence Payload (ASIP) Family of Sensors

Airborne Warning and Control System Block 40/45 Computer and Display Upgrade

B-2 Defensive Management System Modernization (DMS)

B-2 Extremely High Frequency (EHF) SATCOM

B61 Mod 12 Life Extension Program

Battle Control System - Fixed (BCS-F) 3.2

C-130J - HERCULES Cargo Aircraft Program

Cobra Judy Replacement Mission Planning Tool

Combat Rescue Helicopter (CRH)

Command and Control Air Operations Suite (C2AOS)/Command and Control Information Services (C2IS) (Upgrade to AOC applications software suite)

CV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey

Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B

ECSS - Expeditionary Combat Support system

Enclave Control Node (ECN)

EPS - Enhanced Polar System

F-15 Eagle Passive Active Warning Survivability System

F-22 - RAPTOR Advanced Tactical Fighter

F-35 - Lightning II Joint Strike Fighter (JSF) Program

FAB-T - Family of beyond Line-of-Sight Terminals

Full Scale Aerial Target

GBS - Global Broadcast Service

Geosynchronous Space Situational Awareness Program

GPS OCX - Global Positioning Satellite Next Generation Control Segment

GPS-IIIA - Global Positioning Satellite III

Ground Based Strategic Deterrent

Hard Target Munition

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Integrated Strategic Planning and Analysis Network (ISPAN) Increment 4

Joint Air-to-Surface Standoff Missile Extended Range

Joint Space Operations Center Mission System (JMS)

Joint Surveillance Target Attack Radar System (JSTARS) Recapitalization (Recap)

KC-46 - Tanker Replacement Program

Long Range Stand Off (LRSO) Weapon

Long Range Strike Bomber

Massive Ordnance Penetrator (MOP)

Military GPS User Equipment (GPS MGUE)

Miniature Air Launched Decoy-Jammer (MALD-J)

MQ-9 REAPER - Unmanned Aircraft System

NAVSTAR Global Positioning System (GPS) (Includes Satellites, Control and User Equipment)

AIR FORCE PROGRAMS (continued)

Nuclear Planning and Execution System
Presidential Aircraft Recapitalization
Presidential National Voice Conferencing
Protected Tactical Enterprise Service
RQ-4B Block 30 - High Altitude Endurance Unmanned Aircraft System
SBIRS HIGH - Space-Based Infrared System Program, High Component
SBSS B10 Follow-on - Space-Based Space Surveillance Block 10 Follow-on
SF - Space Fence
Small Diameter Bomb, Increment II
Three-Dimensional Expeditionary Long-Range Radar (3DELRR)
Weather Satellite Follow-on (WSF)
Wide Area Surveillance (WAS) Program

Problem Discovery Affecting OT&E

Operational testing of acquisition programs frequently identifies new and significant problems missed in earlier phases of program development, but it can also find problems known prior to operational testing that were unaddressed. The latter is especially problematic, as delays in addressing these problems only exacerbate the cost and time required to fix them. Since 2011, my annual reports have documented both types of problems and the extent to which they exist in programs undergoing operational tests. This year, as in previous years, examples of both were present. Highlighting each of these types of problems is valuable, as the different natures of these types offer insights into the actions needed to field weapons that work.

Discovering problems during operational testing is crucial so they can be fixed prior to system deployment and use in combat. In many cases, an operational environment or user is necessary to uncover the problem. For example, operational aircraft were necessary for the Integrated Defensive Electronic Countermeasures (IDECM) program to discover an unknown hardware problem with the environmental control system, which led to cabin pressurization problems in operationally representative F/A-18C/D aircraft. This problem could not have been discovered in earlier test phases because they used modified developmental aircraft that did not have fully representative hardware. In contrast, the Littoral Combat Ship (LCS) has known problems with the propulsion and power generation systems installed on both variants that continue to affect LCS reliability. The Navy observed these problems again during operational testing and, in the case of the *Freedom* variant, caused the testing to be delayed.

The following discussion provides a summary of the significant problems discovered in FY16 during analyses of operational test events. Detailed accounts of the problems can be found in the corresponding individual program articles in this report. I also list 45 programs that presented significant problems during early testing of systems that have a scheduled operational test in the next two fiscal years. If left uncorrected, these problems could negatively affect my evaluation of operational effectiveness, operational suitability, or survivability. At the conclusion of this section, I report on the progress of the significant problems reported in my FY15 Annual Report.

The results of problem discovery in FY16 are shown in Figure 1. There were 131 programs on the DOT&E oversight list with operational test activity conducted and/or planned between FY16 and FY18. Of those, 74 programs had a total of 83 operational tests or DOT&E reports issued in FY16 (some programs had more than one phase of operational testing this year). Almost one-third (25/83) of the operational tests had no significant problems, while more than two-thirds (58/83) revealed problems significant enough to adversely affect my determination of whether the systems were operationally effective, suitable, or survivable. More than 35 percent (30/83) of these operational tests discovered significant problems that were unknown prior to operational testing.

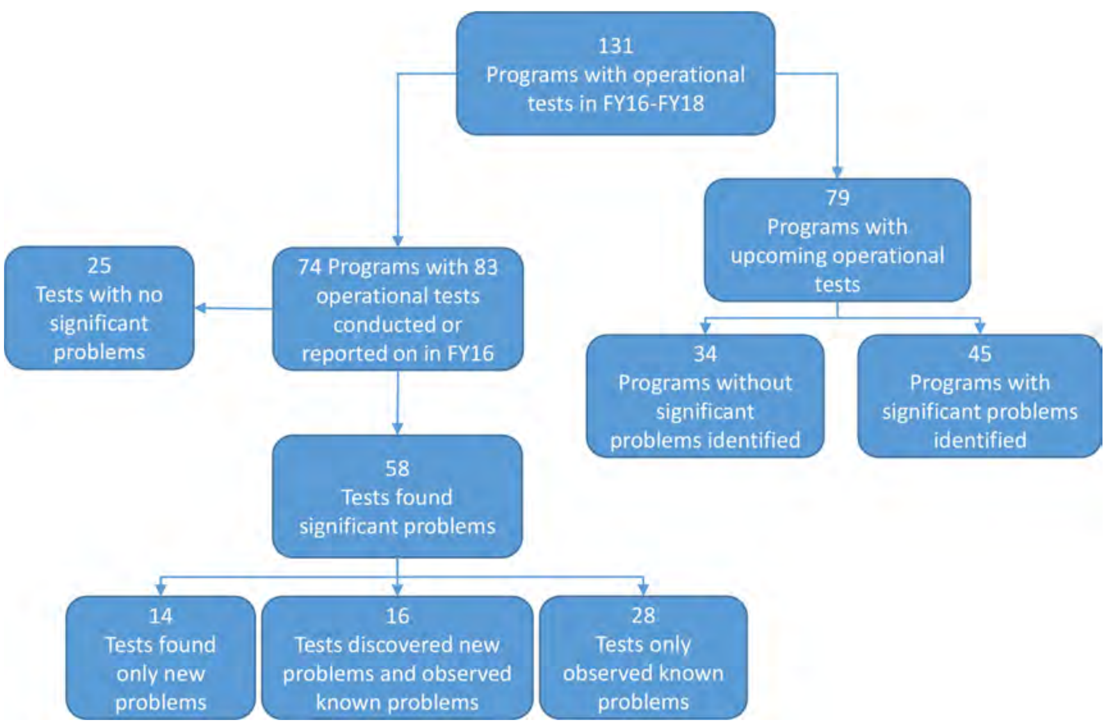


FIGURE 1. PROGRAMS UNDER OVERISGHT WITH OPERATIONAL TESTS IN FY16-FY18
(Note: Programs may have more than one test event between FY16-FY18.)

This year, I identified 179 significant problems across three operational testing areas: effectiveness, suitability, and survivability. Figure 2 shows the distribution of the significant problems found during operational testing by area and whether the problem was known prior to the operational test. Approximately two-thirds of problems (130/179) were known before operational testing. There are several reasons for this. Sometimes the Program Office had already documented a fix for these problems but had not finished implementing it. For example, the Navy discovered a reliability deficiency with the Standard Missile (SM)-6 missile uplink/downlink antennas in developmental testing, but was not able to fix all the missiles before the Block I FOT&E (the anomaly was not observed on any missile with the production fixes during FOT&E). Occasionally, previously documented problems were not considered significant enough to halt progression into the operational test, but the operational test provided new insights that amplified the problem's significance. For example, the Missile Defense Agency concluded that obsolescence changes made between Terminal High-Altitude Area Defense (THAAD) Configuration 1 and Configuration 2 did not affect functionality, but during Flight Test Operational (FTO) - 02, when the full system was integrated, the changes were observed to negatively affect suitability. Other times, a problem was rediscovered that the Program Office thought had already been fixed, such as when LCS-4 experienced disruptions in the flow of navigation data during its operational test. In some cases, the program tried to address the problem but was unable to eliminate it. Examples of this occurred in the CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier, which had low reliability for the Electromagnetic Aircraft Launch System (EMALS) and Advanced Arresting Gear (AAG). The Navy has been addressing known reliability problems in these components, but based on progress to-date, it is unlikely that they will achieve the required reliability without major redesigns.

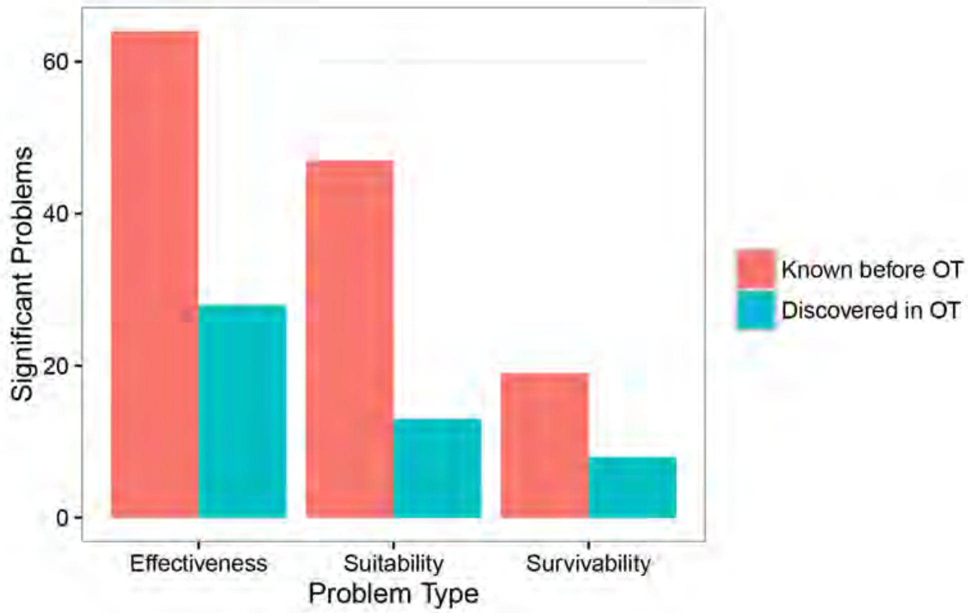


FIGURE 2. BREAKDOWN OF PROBLEMS BY TYPE AND WHETHER THEY WERE KNOWN PRIOR TO OPERATIONAL TESTING

Among the problems discovered in operational testing, the most common reason for finding these problems was the switch to operationally realistic environments and users. During developmental testing of the CV-22 Osprey, the Helmet-Mounted Display Color Display Day Module was only tested in limited environments. The switch to bright sunlight and bright urban conditions in operational testing revealed that the display module actually degraded pilots' situational awareness under such common environments. This problem could have been found in earlier developmental testing had it been tested in operationally representative environments with bright sunlight or in bright urban conditions. In another case, during developmental testing of the AN/SQQ-89A sonar system, the highly skilled users were able to use the system to effectively detect the test torpedoes. However, the operational test revealed that with fleet-representative users this variant of the system (Advanced Capability Build (ACB)-11) did not meet performance metrics, which degrades the effectiveness of torpedo evasion. Fortunately, the Program Office has supported further operational testing and has already documented upgrades to be implemented in a future variant of the system, ACB-15. Limited developmental testing is a common reason that these problems were not discovered prior to operational testing.

Of the problems discovered in operational testing, more than two-thirds (35/49) should have been discovered in developmental testing because they did not require an operationally representative environment to make that discovery. For example, a live test shot of the Advanced Anti-Radiation Guided Missile (AARGM) system revealed flawed logic within the system in the presence of countermeasures, which caused the shot to miss the target. This stopped the operational test and delayed development. Limiting developmental testing and pushing the discovery of these problems into operational testing creates delays in the schedule and increases the costs of development.

All of the survivability problems discovered in operational testing are in the cybersecurity domain (problems discovered during LFT&E are not considered discovered in operational testing). This finding highlights the importance of finding these problems through cybersecurity testing in the operational environment, both to identify and validate cybersecurity vulnerabilities and to assess mission effects and cybersecurity defense effectiveness. Fielding systems with cybersecurity deficiencies can dramatically affect missions and we cannot assume our cybersecurity defenses are up to the task of making up for those deficiencies. Although the details of many of these deficiencies are classified, some explanations of specific problems can be found in the individual program articles in this report.

Figure 3 further breaks down the number of significant problems per operational test by each of the Services.

The LCS systems had large numbers of problems per operational test, with 9 and 13 for the *Freedom* and *Independence* variants, respectively. These problems occurred during FY14-15 operational testing of the two variants that DOT&E reported on in FY16. LCS has continued program development in spite of these problems; of the 22 significant problems, only 2 were discovered in the operational tests. The LCS Program Office has addressed 8 of the remaining 20 known problems. Many of these problems persist because they are inherent to the LCS design; others are fixable but DOT&E is not aware of efforts to correct them. The problems that persist vary from limited fuel range to a design that lacks the redundancy included in other combatants, which could lead to the ship being abandoned in heavy combat situations.

The histograms in Figure 3 show that, in general, the Services experience similar trends in the number of problems observed while conducting operational testing. It is also noteworthy that each of the Services experienced tests with no problems; even in these cases, the operational testing was essential to confirm that users will be able to employ these systems in realistic conditions without being plagued by significant problems.

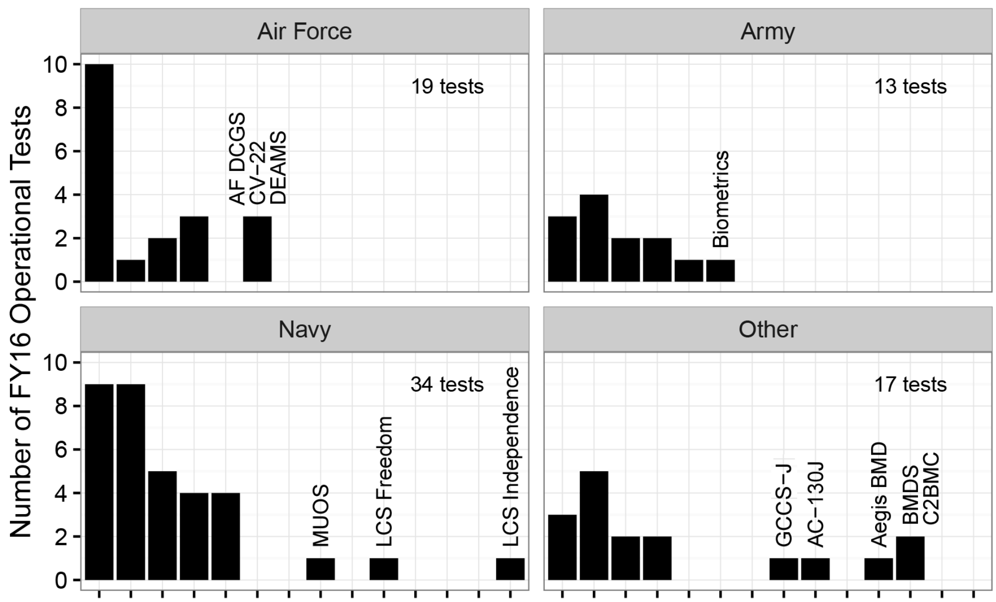


FIGURE 3. HISTOGRAM SHOWING THE NUMBER OF PROBLEMS OBSERVED IN EACH OPERATIONAL TEST, BY SERVICE. PROGRAMS WITH FIVE OR MORE PROBLEMS IN AN OPERATIONAL TEST ARE LABELED.

(Note: The Navy includes the Marine Corps; Other includes the U.S. Special Operations Command, Missile Defense Agency, Defense Logistics Agency, Defense Information Systems Agency, National Security Agency, and Under Secretary of Defense for Personnel and Readiness; the LCS systems labeled above include the surface warfare (SUW) mission package.)

* Problems reported in FY16 for Aegis BMD, BMDS, and C2BMC occurred over 4 years of testing, exaggerating the number of problems per test in this review.

Tables 1 and 2 list the 83 operational tests discussed in this year's Annual Report. Table 1 lists the 25 operational tests that had no significant problems, while Table 2 lists the 58 operational tests that had significant problems. Each row provides the name of the system and operational test, and indicates in which operational testing area problems were observed. For details on the problems observed, see the individual program articles in this report.

TABLE 1. OPERATIONAL TESTS IN FY16 WITH NO SIGNIFICANT PROBLEM DISCOVERY	
System Name	**OT Name**
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) (pg. 341)	AIM-120 Advanced Electronic Protection Improvement Program (AEPIP)
AMRAAM	AIM-120 Electronic Protection Improvement Program (EPIP)
AMRAAM	AIM-120D System Improvement Program (SIP-1) OT
AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) (pg. 201)	AN/BQQ-10 A-RCI Advanced Processing Build 2013 (APB-13) FOT&E
Battle Control System – Fixed (pg. 351)	Battle Control System – Fixed R3.2.3 OT
CHEM DEMIL-ACWA - Chemical Demilitarization Program - Assembled Chemical Weapons Alternatives (pg. 145)	Chemical Demilitarization OT
CHEM DEMIL-ACWA	Explosive Destruction Technology FOT&E
Close-In Weapon System – SeaRAM Variant (pg. 209)	SeaRAM Early Fielding Testing
Consolidated Afloat Networks and Enterprise Services (CANES) (pg. 215)	CANES FOT&E
Defense Agencies Initiative (DAI) (pg. 29)	DAI Operational Assessment Increment 2 Release 1
DAI	DAI Operational Assessment Increment 2 Release 2
Defense Readiness Reporting System – Strategic (DRRS-S) (pg. 37)	DRRS-S IOT&E
E-2D Advanced Hawkeye (AHE) (pg. 237)	E-2D Delta System/Software Configuration Build 2 (DSSC-2) OT-D2
F-22A Advanced Tactical Fighter (pg. 363)	F-22 Update 5 FDE
Geosynchronous Space Situational Awareness Program (GSSAP) (pg. 369)	GSSAP IOT&E
KC-46A Tanker Replacement Program (pg 389)	KC-46A OA-2
LHA 6 New Amphibious Assault Ship (pg 253)	LHA 6 IOT&E
Littoral Combat Ship (LCS) surface warfare (SUW) mission package on *Freedom* variant (pg 257)	OT-C1 *Freedom* variant LCS with Increment 2 SUW mission package
Logistics Modernization Program (LMP) (pg. 161)	LMP IOT&E
Massive Ordnance Penetrator (MOP) (pg. 389)	MOP Enhanced Threat Reduction Phase 3 (ETR-3) Quick Reaction Assessment
Miniature Air-Launched Decoy (MALD) and MALD – Jammer (MALD-J) (pg. 391)	MALD-J FDE
MV-22 Osprey (pg. 299)	MV-22 OT-IIIK Phase 2
Next Generation Jammer (NGJ) Increment One (pg. 301)	NGJ Increment 1 EOA
RQ-4B Global Hawk Block 40 (pg. 399)	RQ-4B Global Hawk Block 40 IOT&E
SSN 774 *Virginia* Class Submarine (pg. 321)	*Virginia* class Block III FOT&E
EOA – Early Operational Test FDE – Force Development Evaluation FOT&E – Follow-on Operational Test and Evaluation	IOT&E – Initial Operational Test and Evaluation OA – Operational Assessment OT – Operational Test

TABLE 2. OPERATIONAL TESTS IN FY16 WITH DISCOVERY OF SIGNIFICANT PROBLEMS				
System Name	**Operational Test**	**Effectiveness**	**Suitability**	**Survivability**
AC-130J Gunship (pg. 337)	AC-130J Block 10 OUE	X	X	
Aegis Ballistic Missile Defense (Aegis BMD) (pg. 413)	Flight Test Operational-02 (FTO-02)	X	X	X
Aegis Modernization Program (pg. 187)	Aegis Baseline Upgrade OT	X	X	X
AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) (pg. 191)	AARGM Block 1 FOT&E	X	X	
Air Force Distributed Common Ground System (AF DCGS) (pg. 343)	AF DCGS Geospatial Intelligence Baseline (GB) 4.1 FDE Phases 2 and 3 and GEOINT Workflow Enhancement (GWE) OUE Phase 1	X	X	
AF DCGS	AF DCGS Systems Release (SR) 3.0 OUE	X	X	X
Air Operations Center – Weapon System (AOC-WS) 10.0 & 10.1 (pg. 345)	AOC-WS 10.1 out-of-cycle (OOC) 13.1	X		
AOC-WS 10.0 & 10.1	AOC-WS 10.1 OOC 13.2			X
AN/BLQ-10 Submarine Electronics Support Warfare Measures (pg. 199)	Technical Insertion 10 (TI-10) FOT&E	X	X	
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite (pg. 203)	AN/SQQ-89A(V)15 Advanced Capability Build 2011 (ACB-11) FOT&E	X	X	
APR-39 D(V)2 (pg. 197)	Army APR-39 D(V)2 FOT&E	X	X	
Army Integrated Air and Missile Defense (AIAMD) (pg. 143)	AIAMD LUT	X	X	
Ballistic Missile Defense System (BMDS) (pg. 405)	Flight Test Operational (FTO) - 02	X	X	
BMDS Sensors / Command and Control (pg. 409)	FTO - 02	X	X	
Biometrics (pg. 171)	Near Real Time Identity Operations (NRTIO) OA	X	X	
Command Web (pg. 147)	Command Web LUT	X		X
Common Aviation Command and Control System (CAC2S) (pg. 211)	CAC2S IOT&E			X
Cooperative Engagement Capability (CEC) (pg. 217)	CEC FOT&E	X		
CV-22 Osprey (pg. 353)	CV-22 OT on the Tactical Software Suite	X	X	X
CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier (pg. 219)	OT-B4 OA	X	X	
Defense Enterprise Accounting and Management System (DEAMS) (pg. 355)	DEAMS Verification of Fixes	X		X
Defense Medical Information Exchange (DMIX) (pg. 33)	MOT&E	X		
Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM) Advanced Threat Warning System (pg 233)	DON LAIRCM FOT&E on the CH-53		X	
Distributed Common Ground System – Army (DCGS-A) (pg. 149)	FOT&E			X
Distributed Common Ground System – Navy (DCGS-N) (pg. 235)	Increment 1, Block 2 FOT&E			X
Expeditionary Transfer Dock and Expeditionary Mobile Base (pg. 239)	Expeditionary Sea Base Class ship IOT&E			X
Global Broadcast Service (GBS) (pg. 371)	GBS FOT&E-1		X	X
Global Command and Control System – Joint (GCCS-J) (pg. 107)	GCCS-J v4.3 Update 1 Emergency Release 1 Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment			X
GCCS-J	GCCS-J Global v6.0 and Agile Client Release 7, v5.1.0.1 OA	X	X	
GCCS-J	GCCS-J Joint Operation Planning and Execution System (JOPES) 4.2.0.4 OT	X		
Ground-based Midcourse Defense (GMD) (pg. 419)	GMD Control Test Vehicle-02+ (CTV-02+)		X	X
Infrared Search and Track (IRST) (pg. 247)	F/A-18 Block I Operational Assessment 2 (OA-2)	X	X	
Integrated Defensive Electronic Countermeasures (IDECM) (pg. 249)	IDECM Integrated DT/OT	X	X	

TABLE 2. OPERATIONAL TESTS IN FY16 WITH DISCOVERY OF SIGNIFICANT PROBLEMS (CONTINUED)				
System Name	**Operational Test**	**Effectiveness**	**Suitability**	**Survivability**
Javelin Close Combat Missile System – Medium (pg. 153)	Javelin Spiral 2 - Live Fire Test Program	X		
Joint Standoff Weapon (JSOW) (pg. 251)	JSOW C-1 FOT&E	X		
Joint Tactical Network (pg. 157)	Joint Enterprise Network Manager (JENM) Early Fielding with Mid-Tier Networking Vehicular Radio (MNVR)	X		
Joint Warning and Reporting Network (JWARN) (pg. 115)	JWARN Increment 2 IOT&E A-1		X	X
Littoral Combat Ship (LCS) seaframe, *Freedom* variant (pg. 257)	OT-C1 *Freedom* variant LCS with Increment 2 surface warfare (SUW) mission package	X	X	X
LCS seaframe, *Independence* variant	OT-C4 *Independence* variant with Increment 2 SUW mission package	X	X	X
LCS SUW mission package on *Independence* variant	OT-C4 *Independence* variant with Increment 2 SUW mission package	X	X	
Mid-tier Networking Vehicular Radio (MNVR) (pg. 167)	MNVR OA	X		
Mobile User Objective System (MUOS) (pg. 289)	MUOS MOT&E-2	X	X	
MQ-4C Triton (pg. 293)	MQ-4C Triton OA	X		
MQ-8 Fire Scout Unmanned Aircraft System (pg. 295)	MQ-8C Fire Scout Milestone C OA	X		
MQ-9 Reaper (pg. 393)	MQ-9 Reaper Block 5 FOT&E	X	X	
Next Generation Diagnostic System (NGSD) Increment 1 (pg. 121)	NGDS OA		X	
P-8A Poseidon (pg. 303)	P-8A Data Storage Architecture Upgrade (DSAU) / VCD FOT&E		X	X
P-8A Poseidon Multi-Mission Aircraft (MMA)	P-8A Poseidon MMA Increment 2 Engineering Change Proposal 2 (ECP-2)	X		
Public Key Infrastructure (PKI) Increment 2 (pg. 123)	PKI Increment 2 Token Management System (TMS) Release 4 LUT	X	X	
Rolling Airframe Missile (RAM) Block 2 (pg. 311)	RAM Block 2 IOT&E	X		
Soldier Protection System (SPS) (pg. 177)	SPS IOT	X		
Space-Based Infrared System Program, High Component (SBIRS High) (pg. 403)	SBIRS Block 10 OUE		X	
Spider Increment 1A M7E1 Network Command Munition (pg. 181)	Spider Increment 1A LUT	X	X	X
Standard Missile-6 (SM-6) (pg. 323)	SM-6 Block I FOT&E	X		
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 (pg. 327)	SEWIP Block 2 IOT&E	X		
Terminal High-Altitude Area Defense (THAAD) (pg. 421)	Flight Test Operational (FTO) - 02	X		
Theater Medical Information Program – Joint (TMIP-J) (pg. 127)	TMIP-J I2R3 MOT&E	X		X
Warfighter Information Network – Tactical (WIN-T) (pg. 183)	WIN-T Increment 3 OA	X		X

DT/OT – Developmental Test/Operational Test
FDE – Force Development Evaluation
FOT&E – Follow-on Operational Test and Evaluation
IOT – Initial Operational Test
IOT&E – Initial Operational Test and Evaluation
LUT – Limited User Test
MOT&E – Multi-Service Operational Test and Evaluation
OA – Operational Assessment
OT – Operational Test
OUE – Operational Utility Evaluation
VCD – Verification of Correction of Deficiencies

There are 79 programs that have operational tests scheduled to begin in the next two fiscal years, and I am aware of significant problems that, if not corrected, could adversely affect my evaluation of the effectiveness, suitability, or survivability of 45 of these systems. Table 3 lists the upcoming operational tests for systems discussed in this year's Annual Report (see individual program articles in this report for details on the problems). Table 4 lists the upcoming operational tests for systems that do not have entries in this year's report. For these systems, brief descriptions of the problems are provided after the table.

TABLE 3. PROGRAMS IN THIS ANNUAL REPORT WITH PROBLEMS THAT MAY ADVERSELY AFFECT UPCOMING OPERATIONAL TESTING				
System Name	**Upcoming Test**	**Effectiveness**	**Suitability**	**Survivability**
AC-130J Gunship (pg. 337)	AC-130J IOT&E	X	X	
Aegis Ballistic Missile Defense (Aegis BMD) (pg.413)	Flight Test Operational-03 (FTO-03)	X	X	
AH-64E Apache (pg. 141)	AH-64E Apache (Version 6) FOT&E II		X	
Air Force Distributed Common Ground System (AF DCGS) (pg. 343)	AF DCGS Systems Release (SR) 3.0.1 IOT&E	X	X	X
Air Operations Center – Weapon System (AOC-WS) 10.0 & 10.1 (pg. 345)	AOC-WS 10.1 out-of-cycle (OOC) 13.3	X		
AOC-WS 10.2	AOC-WS 10.2 OA	X		
Airborne Warning and Control System (AWACS) (pg.359)	E-3 AWACS Block 40/45 FOT&E	X	X	X
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite (pg. 203)	AN/SQQ-89A(V)15 Advanced Capability Build 2011 (ACB-11) FOT&E	X	X	
APR-39 D(V)2 (pg. 197)	Army APR-39 D(V) 2 FOT&E	X	X	
Army Integrated Air and Missile Defense (AIAMD) (pg. 143)	AIAMD OA for Milestone C Decision	X	X	
Ballistic Missile Defense System (BMDS) (pg. 405)	Flight Test Operational-03 (FTO-03)	X	X	
CH-53K (pg. 205)	CH-53K OT-B1	X	X	
Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I (pg. 257) (LCS)	COBRA Block I Phase I IOT&E	X		
Command and Control, Battle Management, and Communications (C2BMC) (pg. 409)	Flight Test Operational-03 (FTO-03)	X	X	
Cooperative Engagement Capability (CEC) (pg. 217)	CEC FOT&E	X		
Defense Enterprise Accounting and Management System (DEAMS) (pg. 355)	DEAMS FOT&E	X	X	X
Defense Medical Information Exchange (DMIX) (pg. 33)	DHMSM IOT&E	X		
Department of Defense Healthcare Management System Modernization (DHMSM) (pg. 43)	DHMSM IOT&E	X		X
F-22A Advanced Tactical Fighter (pg. 363)	F-22A Increment 3.2B IOT&E	X		
F-35 Lightning II Joint Strike Fighter (JSF) (pg. 47)	JSF Block 3F IOT&E	X	X	X
F/A-18 E/F Super Hornet Naval Strike Fighter and EA-18G Airborne Electronic Attack (pg. 243)	H12 OT	X	X	
Family of Advanced Beyond Line of Sight Terminal (FAB-T) (pg. 367)	FAB-T Command Post Terminal (CPT) IOT&E	X		
Geosynchronous Space Situational Awareness Program (GSSAP) (pg. 369)	FOT&E 1	X		X
Global Command and Control System – Joint (GCCS-J) (pg. 107)	GCCS-J Global OA	X	X	X
Global Positioning System (GPS) Enterprise (pg. 375)	Military GPS User Equipment (MGUE) Increment 1 OA	X		
Ground-based Midcourse Defense (GMD) (pg. 419)	Flight Test GMD-15 (FTG-15)	X	X	
Integrated Defensive Electronic Countermeasures (IDECM) (pg. 249)	IDECM Software Improvement Program (SWIP) FOT&E	X	X	
Joint Information Environment (JIE) (pg. 111)	JIE OA	X	X	
Joint Space Operations Center Mission System (JMS) (pg. 381)	JMS Increment 2, Service Pack 9 OUE	X		
Joint Warning and Reporting Network (JWARN) (pg. 115)	JWARN Increment 2 Requirements Definition Package (RDP) 2 Capability Drop 2.1		X	
KC-46A (pg. 385)	KC-46A IOT&E	X		
Key Management Infrastructure (KMI) (pg. 117)	Spiral 2, Spin 2 OA	X		
M109A7 Paladin Integrated Management (PIM) (pg. 165)	M109A7 PIM IOT&E	X	X	
MQ-4C Triton Unmanned Aircraft System (UAS) (pg. 293)	MQ-4C Early Fielding Evaluation for Integrated Functional Capability (IFC) 3.1	X		
Next Generation Diagnostic System (NGDS) (pg. 121)	NGDS MOT&E		X	
P-8A Poseidon Multi-Mission Aircraft (MMA) (pg. 303)	P-8A Increment 2 Engineering Change Proposal 2 (ECP-2)	X		
Patriot Advanced Capability-3 (PAC-3) (pg. 173)	Patriot Post-Deployment Build-8 and Missile Segment Enhancement IOT&E	X	X	X
Spider (pg. 181)	Spider I1A IOT&E	X	X	
Surface Mine Countermeasures Unmanned Undersea Vehicle (SMCM UUV) (pg. 257)	Knifefish OA	X	X	
Surface Ship Torpedo Defense (SSTD) Torpedo Warning System (TWS) Countermeasure Anti-Torpedo (CAT) (pg. 329)	QRA and Early Fielding Report Update	X		

TABLE 3. PROGRAMS IN THIS ANNUAL REPORT WITH PROBLEMS THAT MAY ADVERSELY AFFECT UPCOMING OPERATIONAL TESTING (CONTINUED)				
System Name	**Upcoming Test**	**Effectiveness**	**Suitability**	**Survivability**
Terminal High-Altitude Area Defense (THAAD) (pg. 421)	Flight Test THAAD-18 (FTT-18)	X	X	X
Virginia Class Block III Submarine (pg. 321)	*Virginia* Block III FOT&E		X	
Warfighter Information Network – Tactical (WIN-T) (pg. 183)	WIN-T INC2 FOT&E	X		X
FOT&E - Follow-on Test and Evaluation IOT&E – Initial Operational Test and Evaluation MOT&E – Multi-Service Operational Test and Evaluation OA – Operational Assessment	OT – Operational Test OT&E – Operational Test and Evaluation OUE – Operational Utility Evaluation QRA – Quick Reaction Assessment			

TABLE 4. PROGRAMS NOT IN THIS ANNUAL REPORT WITH PROBLEMS THAT MAY ADVERSELY AFFECT UPCOMING OPERATIONAL TESTING				
System Name	**Upcoming Test**	**Effectiveness**	**Suitability**	**Survivability**
Nett Warrior	Nett Warrior LUT	X		
Common Analytical Laboratory System (CALS)	CALS Field Confirmatory (FC) Analytical Capability Sets (ACS) User Demonstration	X	X	
LUT – Limited User Test				

Nett Warrior. Nett Warrior is a dismounted leader situational awareness system for use during combat operations.

- Nett Warrior's effectiveness when used dismounted at the company-level was adversely affected by Manpack radio's low message completion rate of position location information. The Program Office has implemented a fix but it has not been operationally tested.

Common Analytical Laboratory System (CALS). CALS provides sensors for the identification of chemical and biological agents in environmental samples.

- During testing at operationally realistic high and low temperatures, the HAPSITE® ER Gas Chromatograph/Mass Spectrometer was unable to pass its internal performance verification step.
- During the developmental/operational testing, routine handling of the HAPSITE® ER by test operators resulted in scratches to the instrument screen on the primary and spare systems causing the systems to fail. A scratch on the screen creates an error message that requires factory level maintenance and, in some cases, entire reprogramming of the instrument by the vendor.
- The CALS Analytical Capability Set Biological Subsystem includes the NIDS® Lateral Flow Immunoassay system, which performed poorly and experienced reliability problems during confidence checks in environmental developmental testing.

PROGRESS UPDATES ON PROBLEMS REPORTED IN THE FY15 ANNUAL REPORT

In my annual report last year, I identified 8 systems that discovered only new problems, 19 systems that discovered new problems and re-observed known problems, and 18 systems that only re-observed known problems during operational testing in FY15. The status of these 45 programs is listed below.

All fixes implemented and verified in OT (6/45)

- Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) for AN/BQQ-10(V) Sonar
- F-22A Advanced Tactical Fighter
- LHA 6 New Amphibious Assault Ship
- Miniature Air-Launched Decoy – Jammer (MALD-J)
- Mobile Landing Platform (MLP) Core Capability Set (CCS) (Expeditionary Transfer Dock) and Afloat Forward Staging Base (AFSB) (Expeditionary Mobile Base)
- MV-22 Osprey

Some (or all) fixes implemented but new problems discovered or known problems re-observed in OT (21/45)

- AC-130J Ghostrider
- Aegis Modernization Program
- Air Force Distributed Common Ground System (AF DCGS)
- AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite
- Air Operations Center – Weapon System (AOC-WS) 10.0 & 10.1
- Ballistic Missile Defense System (BMDS)

- CV-22 Osprey
- CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier
- Defense Enterprise Accounting and Management System (DEAMS)
- Defense Medical Information Exchange (DMIX)
- Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM)
- Global Command and Control System – Joint (GCCS-J)
- Integrated Defensive Electronic Countermeasures (IDECM)
- Infrared Search and Track (IRST)
- Joint Warning and Reporting Network (JWARN)
- Littoral Combat Ship (LCS) *Freedom* Class
- LCS *Independence* Class
- Mid-Tier Networking Vehicular Radio (MNVR)
- P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)
- Surface Electronic Warfare Improvement Program (SEWIP) Block 2
- Warfighter Information Network – Tactical (WIN-T)

Some fixes (potentially) implemented; currently in OT or planning additional OT (10/45)

- Countermeasure Anti-Torpedo (CAT)
- F/A-18E/F Super Hornet
- Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)
- Guided Multiple Launch Rocket System – Alternate Warhead (GMLRS-AW)
- Key Management Infrastructure (KMI) Increment 2
- MQ-1C Unmanned Aircraft System (UAS) Gray Eagle
- Q-53 Counterfire Target Acquisition Radar System
- Ship Self-Defense System (SSDS)
- Torpedo Warning System (TWS)
- *Virginia* Class Block III Submarine

No fixes planned, or no fixes planned to be tested in the next two years (8/45)

- AIM-9X Air-to-Air Missile Upgrade
- Airborne Mine Neutralization System (AMNS)
- Integrated Personnel and Pay System – Army (IPPS-A)
- Global Combat Support System – Marine Corps (GCSS-MC)
- H-1 Upgrades to AH-1Z Attack Helicopter and UH-1Y Utility Helicopter
- Joint High Speed Vessel (JHSV)
- MH-60R Multi-Mission Helicopter
- Surveillance Towed Array Sensor System (SURTASS) and Compact Low Frequency Active (CLFA) Sonar

In FY15, I also identified 48 systems that had significant problems in early testing that should be corrected before operational testing. The following provides an update on the progress these systems made in implementing fixes to those problems.

Fixes verified in OT - No other problems observed (2/48)

- Acoustic Rapid Commercial Off -the-Shelf Insertion (A-RCI) for AN/BQQ-10(V) Sonar
- F-22A Advanced Tactical Fighter

Fixes verified in OT - New problems observed (2/48)

- Defense Medical Information Exchange (DMIX)
- P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)

Fixes verified in OT - Known problems re-discovered (8/48)

- AN/BLQ-10 Submarine Electronic Support System
- Defense Enterprise Accounting and Management System (DEAMS)
- Department of the Navy Large Infrared Countermeasures (DON LAIRCM)
- Infrared Search and Track (IRST)
- Mid-Tier Networking Vehicular Radio (MNVR)
- MQ-4C Triton Unmanned Aircraft System (UAS)
- Mobile User Objective System (MUOS)
- Surface Electronic Warfare Improvement Program (SEWIP) Block 2

Fixes tested in OT - Both new problems discovered and known problems re-observed (11/48)

- AC-130J Ghostrider
- Aegis Modernization
- Air Force Distributed Common Ground System (AF DCGS)
- AGM-88E Advanced Anti-Radiation Guided Missile (AARGM)
- AN/SQQ-89A(V) Integrated Undersea Warfare (USW) Combat Systems Suite
- CV-22 Osprey
- Global Command and Control System – Joint (GCCS-J)
- Integrated Defensive Electronic Countermeasures (IDECM)
- Littoral Combat Ship (LCS) *Independence* Class
- MQ-9 Reaper Armed Unmanned Aircraft System (UAS)
- Warfighter Information Network – Tactical (WIN-T)

Fixes not planned to be tested in the next two years (10/48)

- Airborne Laser Mine Detection System (ALMDS)
- Airborne Mine Neutralization System (AMNS)
- Air Operations Center – Weapon System (AOC-WS) 10.2
- DOD Automated Biometric Identification System (ABIS)
- Mark XIIA Mode 5 Identification Friend or Foe (IFF)
- Integrated Personnel and Pay System – Army (IPPS-A) Increment II
- Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS)
- Joint Battle Command – Platform
- MK 54 Lightweight Torpedo
- Remote Minehunting System (RMS)

Fixes currently being tested or planned to be tested in the next two years (15/48)

- AH-64E
- Ballistic Missile Defense System (BMDS)
- CH-53K Heavy Lift Replacement Program
- Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I
- Countermeasure Anti-Torpedo (CAT)
- F/A-18E/F Super Hornet
- Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)
- Key Management Infrastructure (KMI)
- Military GPS User Equipment (MGUE)
- Nett Warrior
- GPS Next Generation Operational Control System (OCX)
- Patriot Advanced Capability-3 (PAC-3)
- Torpedo Warning System (TWS)
- *Virginia* Class Block III Submarine
- XM25 Tactical Increment 2 XM 25 Counter Defilade Target Engagement System (CDTE)

DOD Programs

Major Automated Information System (MAIS) Best Practices

Introduction

DOT&E oversees operational testing of 30 DOD Major Automated Information Systems (MAIS) programs.[1] Many MAIS program managers find it challenging to meet cost, schedule, and performance goals. The U.S. Government Accountability Office (GAO) reported in 2014 that, "most selected [MAIS] programs changed their planned cost and schedule estimates, and over half did not fully meet system performance targets."[2] The same report stated that of the 15 MAIS programs the GAO studied, "three of the selected programs reported meeting system performance targets, while eight reported not fully meeting targets, and four did not have system performance data available." All of the 15 programs that GAO reviewed are on the DOT&E oversight list, and DOT&E has gained unique insights into MAIS programs through operational testing.

The purpose of this section is to identify best practices in MAIS acquisition and provide examples of how those were implemented by the systems under DOT&E oversight. The DOD acquisition workforce has sporadically implemented many of the best practices for MAIS programs. A wider, more consistent application of the best practices described in this section, including implementation of an agile acquisition framework, should help DOD more frequently deliver successful MAIS programs that perform well during operational testing and in the field.

Challenges

The challenging nature of MAIS acquisition can be attributed to many factors, but software acquisition reference materials often cite complexity and unstable requirements as the most significant.

- Program complexity. DOD MAIS programs tend to be very complex. Typical MAIS programs have to be integrated into multiple existing enterprises that contain large numbers of interfaces with government and commercial entities, each with its own configuration, database structure, and security requirements. In addition, the program itself most often is an integration of large numbers of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) components with existing military and commercial networks. This complexity is often paired with an acquisition strategy that requires delivery of a full, mature product in a single development cycle, which often results in delays and performance shortfalls.
- Unstable requirements. DOD systems often have to deal with changing requirements. In many cases, the changes are driven by advancement in technology (e.g., vendors updating hardware, operating system, or database versions) and the program office must either pay sharply increased costs to continue the support or move to the new version with associated changes. At other times, world events and doctrine changes drive the requirements to change (e.g., a system that was intended for use in conventional warfare may need new functions to be used in counterinsurgency warfare). In either case, changes in requirements necessitate changes in software, causing disruptions in the development cycle.

Best Practices

These challenges may be mitigated through MAIS program best practices. In the process of overseeing the operational testing of systems under DOT&E oversight, DOT&E noted the following 10 practices that produced observable benefits to the programs.

Robust Senior-Level Participation

Robust and continued senior-level attention and participation contributed significantly to the success of agile acquisition MAIS programs like the Army's Logistics Modernization Program (LMP), Global Combat Support System – Army (GCSS-A), and GCSS – Joint (GCSS J). Senior leader support was key for securing necessary resources, enforcing updated business processes, and shortening decision cycles.

- Resource help. Agile programs tend to have relatively short delivery cycles. This often means short development-test-deployment cycles. Executing such agile cycles is resource-intensive for the entire acquisition team. A typical agile program deploys an approved release, develops the current release, and plans for the next release, all at the same time. To support such concurrent acquisition cycles, testers must simultaneously prepare evaluation reports from the last release, execute and witness test events for the current release, and conduct risk assessment and plan test events for the next release. One test team usually cannot adequately plan test, and report simultaneously. To reduce the burden, the GCSS-J Program Office provided sufficient resources to form two

1 Section 2445a of title 10, U.S. Code, defines a MAIS program as a DOD information technology (IT) investment with: 1) program costs in any single year exceeding $32 Million; 2) total program acquisition costs exceeding $126 Million; or 3) total life-cycle costs exceeding $378 Million (all in FY00 constant dollars). DOD Instruction (DODI) 5000.02, "Operation of the Defense Acquisition System," dated January 7, 2015, updates the dollar figures to FY14 constant dollars: 1) $40 Million in any single year, 2) $165 Million total program cost, or 3) $520 Million total life-cycle cost. The Secretary of Defense and the Milestone Decision Authority can also use discretion to designate a program as a MAIS.

2 GAO report GAO-14-309, "Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practices," March 27, 2014, page 16

test teams so that each team could alternate and focus on one release at a time.

- Enforcement of updated business processes. Users tend to be comfortable with the business processes or tactics, techniques, and procedures (TTPs) they have been using. Unfortunately, new TTPs and business processes are inevitable with significantly new capabilities for a couple of reasons. First, new software often will not support established business processes and TTPs without customization, and the risk in a MAIS program tends to correspond to the amount of customization. Customization can cause deviation from the initial design of the COTS and GOTS software. Such a change necessitates not only new code writing, but also may change the way the software interfaces with other systems or modules. Second, the use of outdated business processes and TTPs increases the risk of not using the new software to its maximum value. The advantages of automation are eliminating manual steps and reducing human decision points. Some users might resist such automation, but avoiding automation can negate the benefit of the new technology. Thus, once decision-makers agree there is a need to change TTPs and business practices, they must help implement them by enforcing their use and providing the necessary resources for training. The Army's LMP performed well during its recent operational test in part because of the rigorous user training the program manager provided well prior to the test.
- Shortened decision cycles. The acquisition process for MAIS programs require OSD-level decisions, which can often mean lengthy staffing processes. This is very difficult for programs that deploy more than one release per year. Many programs successfully developed a model where they adequately informed decision-makers without lengthy staffing processes. One such method is simultaneous staffing of acquisition decisions vice a step-by-step iteration of signature process. This method is not always practical, but can work well if senior-level leaders participate in the acquisition. For instance, LMP Increment 2 grouped seven releases into three waves. Each wave grouped one to three releases based on a risk assessment. The acquisition decision makers made production and fielding decisions for waves rather than individual releases. This way, decision makers still managed risks without excessive, time-consuming staffing processes.

Flexible and Disciplined Requirements Management

Program sponsors for the majority of MAIS programs document their requirements with the Joint Capabilities Integration Development System "IT Box" model. With the IT Box, requirements are specified in an Information System Initial Capability Document (IS ICD) and Information System Capability Development Document (IS CDD).[3] The program sponsors describe more details of the IS ICD and IS CDD requirements in Requirements Definition Packages and further define the capability for each release in Capability Drops.[4]

One advantage of agile acquisition and the IT Box is the flexibility to adjust the priority and urgency of requirements. Program sponsors document requirements at the beginning of the acquisition program when the software developers and users know only a rough outline of the program. As the system matures, users and developers might realize some of the requirements are not consistent with the best use of the system's capabilities. The threats or the doctrine may change, and in response, the program may need to develop a capability earlier than originally planned. A software module might encounter significant challenges that could ultimately influence the acquisition timeline. In such cases, the IT Box provides the requirement governance body with the authority to decide whether to leave that capability for a future release, or to add resources to complete that capability.

Many MAIS programs implement commercially available agile framework products. Most agile frameworks state requirements in terms of user stories, which are a small segment of functionality that a user wants. The capability to execute a user story is delivered in a sprint, or a small segment of software. The user stories are combined into an epic, which is a larger description of how the user intends to use the system. The capability to execute the epic is delivered in a release composed of multiple sprints.

Compared with typical requirements in a system specification such as "system ABC must be able to perform XXX task within YY seconds," epics and user stories provide a more operational context such as "the user must be able to receive X input and produce Y product in time to support Z task."[5] The user story not only provides performance goals for each task, but also provides operational context of how those tasks work together to produce a desired outcome.

A user story allows the program sponsor to frame a feature in terms of its benefits for a particular user. A well-written user story helps developers design software that delivers specific benefits. A pitfall a program can easily fall into is breaking epics into tasks rather than user stories. In those cases, development and testing processes becomes task-focused (doing things) instead of delivery-focused (creating value). For a coherent and consistent understanding of requirements in operationally relevant terms, it is important to describe requirements in terms of value to the user rather than tasks; e.g., a user story should be, "user must update unit location before the next planning update cycle," rather than, "user must be able to update the unit location in less than 4 seconds." This way, developers and testers can both understand the importance and operational consequence of each step.

---

3 Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), February 12, 2015, page D-29

4 Ibid., page D-34 and figure D-4

5 Defense Acquisition University (https://dap.dau.mil/glossary/Pages/2752.aspx) defines system specification as "a description of the system-level requirements, constraints, and interfaces (functional, performance, and design) and the qualification conditions and procedures for their testing and acceptance. The System Specification, initially reviewed at the System Requirements Review (SRR), ultimately becomes part of the functional baseline that is confirmed at the completion of the System Functional Review (SFR)."

For the Distributed Common Ground System – Army (DCGS-A) FOT&E, DOT&E evaluated the system primarily based on the user's ability to execute "vignettes" – a series of user actions that accomplishes the mission. For instance, one of the vignettes required the brigade equipped with DCGS-A to identify a facility that manufactured IEDs, and locate and designate the facility to be targeted. The Army program sponsors developed 10 such vignettes for FOT&E. The program sponsor, in concert with combat developers and the brigade, further divided the vignettes into steps for specific DCGS-A users.

Change Management that Starts Early and Continues Throughout the Process

Military users cannot always adapt to commercial practices. In such cases, the program office should work closely with the users to refine business processes. For example, the GCSS – Marine Corps (GCSS-MC) Program Office spent many months with system designers and tactical users, exchanging ideas and designing new business processes that retained the power of new software while accommodating specific military requirements such as limited bandwidth on the move, limited ability to carry heavy hardware, and unit personnel changing over with military rotations. The process was iterative; approved procedures did not always work out the way users and engineers expected. In such cases, users and engineers needed to retune business processes and software to accommodate the military missions.

After deploying the new software, the GCSS-MC Program Office fielding team worked extensively with users during the fielding process so that individual adjustments could be made for specific users. Similarly, another program, GCSS-J, coordinated early with the users to describe their workflow in terms of user stories, and continued dialog with the users after fielding to make requested changes. Such adjustments can be as simple as redesigning the look of the display and writing patches to adapt the software. In some cases, extensive adjustments ended up as a new function to be delivered in the next available software drop, pending approval by decision-makers.

Architecture Description in Accordance with the DOD Architectural Framework

A well-designed and sufficiently detailed architecture is a prerequisite for effective development and employment of enterprise software. This is no different than needing a detailed blueprint for a building before construction and for maintenance. The more complex a program is, the more the developer and maintainers need the architecture description. The DOD architectural framework provides an outline for documenting the architecture.

Sufficiently detailed workflow information (as provided in the system view and operational view architectural products) should be coordinated with users to develop user procedures and training. Such coordination allows discussion regarding how the system can be integrated into user's doctrine and procedures, or to modify the doctrine, procedures, and user training to take advantage of the technology.

During the development and sustainment phases, the program office should update architectural products to ensure consistency with user procedures and updated interfacing systems. The updated architecture should also remain consistent with user stories that describe the updated procedures and interfaces.

Mature Doctrine and Training Development

It is easy to fall into the trap of mistaking the purchase of tools with providing solution to a problem. In reality, tools do not help the user unless users know how to use the tools to accomplish the mission. For DOD systems, successful programs tend to have doctrine that describes how the system fits into the overall military operations. The doctrine in turn becomes the basis of developing TTPs that describes in more detail how the users should employ the functions the system provides. The doctrine and TTPs then should be integrated into a training program so that users have necessary knowledge to operate and maintain the system.

- TTPs. While the program manager should make the transition to a new MAIS program as seamless as possible, the reality of automation and optimization can demand change in the way the military does things. For instance, whereas the old process may have been to place an order for a part first and have the financial office check that order against available funds second, the new software may pre-check the funds balance as a part of processing the order. To take advantage of new capabilities, system sponsors and users must develop and train doctrine and TTPs. GCSS-A incrementally fielded capability with sufficient time to develop the TTPs so that the users received systems with clear instructions on how to use the system to accomplish the mission.
- Training. User training for new system capabilities should include not only how to do an individual task, but also how to work with the new capabilities as a team. The training must include sufficient practice sessions to get used to new TTPs and for each unit to develop its own operating procedures. The DCGS-A Program Manager dedicated almost a year to gradually increasing the scope of training, starting with individual training and culminating in a brigade free-play training exercise.

Iterative Developmental Tests that Start Early

MAIS programs typically have one prime vendor that integrates hardware and software components from multiple vendors. The program office should have a coherent strategy to find and fix problems as each software component is developed and delivered, because software engineers can find and fix problems more quickly before a software module is integrated into a larger and more complex program. Isolating the root causes of a problem can be very difficult after the software has been nested with other vendors' products. In addition, the prime vendor may have to redo the integration work after receiving an updated software module.

Database Interfaces and Commonality

MAIS programs typically ingest data from multiple sources to produce new database products. If data sources provide inaccurate data, the resulting product will be inaccurate. The program may not be able to ingest the data if a data source provides data in a different format. To minimize such risks, the

LMP Program Management Office (PMO) conducted trading partner test (TPT) as well as process and data integrations test (PDIT) events before government developmental test (DT) and operational test (OT) events. The TPT ensured interfaces with trading partner systems worked as intended, and the PDIT ensured that the end-to -end processes worked well. Many programs do adequate interface tests that are similar to a TPT, but they neglect to test an entire process as done in the PDIT. An early test of process and data in a controlled environment makes it much easier to identify and fix root causes of any discrepancies. The TPTs and PDITs provided the LMP PMO early opportunities to discover shortfalls and implement necessary adjustments.

The LMP PMO put management focus on data integration. Conducting PDITs before DT and OT events helped ensure LMP was ready to ingest and use accurate data from the data sources. The PDITs helped LMP avoid one of the most common causes for logistics system failures: nomenclature inconsistencies. For instance, when a user needs to know how many M1A1 tanks are in the unit's inventory, the database should be capable of counting all M1A1s. Unfortunately, one database may call it M1A1; another database may call it Abrams Tank; and another database may call it "tank, main battle, armored." Even worse, some databases may track the data at the component level (such as engine, transmission, or gun mounts) rather than the platform level such as M1A1. Given the variety of source databases, the LMP database manager had to first correlate all of these terms with a common term before the system could return an accurate count for the query. Even when the database manager succeeds in this difficult task, if the database manager is not careful, a query for "Abrams tank" may count all of the M1A2s as well as M1A1s. If the intent was to count M1A1s, the count would be wrong. The database manager must find a way to work with all of the existing databases and either build interfaces or modify databases. LMP managed this challenge by conducting well-designed, two way data integration tests to identify and fix the interface issues.

DCGS-A is an intelligence system that exploits intelligence, surveillance, and reconnaissance data to produce actionable intelligence. The system accomplishes this through an intelligence fusion process that combines information from a large number of sources. The fused intelligence can only be as good as the accuracy of the data it uses. The Army quickly found that synchronizing databases is a daunting challenge and created the Tactical Entity Database (TED) that combines and organizes data from hundreds of sources into specific entities. An entity may be a person, building, organization, or equipment. By organizing large and disparate information into a coherent database, information can be correlated and associated so that an analyst can get a clear picture of what is in the unit's area of responsibility.

Even after the creation of TED, DCGS-A had more database challenges to overcome. In unconventional warfare, the database has to record many items that do not have standard nomenclatures, or item names. An example is a brand new type of IED. For some purposes, such as route planning, the unit would find it more useful to group all such devices as IEDs. For other intelligence purposes, the unit may need to identify specific types of IED, and must create a new item description to document that type of IED. The new nomenclature needs to be designed so that DCGS-A can still recognize it as an IED when a user queries for total number of IEDs. In addition, the creator of the new nomenclature must ensure all other DCGS-A users are aware of such item description. The Army conducted extensive unit-level training to define and teach when to create new nomenclature, how to create the nomenclature, and how to share the new nomenclature with other users.

DCGS-A followed the intelligence fusion process that begins with the fusion level 0, or "Normalization," step. Normalization is the process where DCGS-A users enter data from multiple sources into TED. If a soldier reported seeing a truck with a machine gun mounted in the back, the data entry person would first look to see if such an item is on the pull-down menu. If not, the data entry person must decide whether to create a new item or call it the most similar item such as armored personnel carrier with machine gun. This step determines the value and accuracy of all processes that follow.

DOT&E evaluated DCGS-A to be not operationally effective after the IOT&E in 2012, but evaluated the system to be operationally effective after the FOT&E in 2015. Many factors contributed to the difference, but one of the most significant improvements was TED. A major contributing factor was that the Army conducted a series of extensive training events, including unit-level training, so that the unit was able to develop and train with detailed procedures and processes.

Database accuracy and currency cannot rely on software solutions alone. Proper data integration and interfaces tend to be the most accurate predictors of program success for networked MAIS systems. Accordingly, program managers should first identify and document all database and interface requirements in architectural products, monitor progress via interface and data integration tests, and implement procedures and training programs to ensure users maintain the databases properly.

A Robust Developmental Test with Operationally Representative Interfaces and Networks

Automated developmental testing is critical to gain efficiency and accuracy. Automated acceptance and regression tests provide an efficient and reliable option to verify that a code change works as intended without breaking anything. However, program offices must avoid using automated testing as a replacement for a comprehensive DT. Automated testing is a prerequisite step to make sure coding is done correctly; it is not a validation of the software's ability to support the user's mission.

Many complex MAIS programs perform well in DT and fail to perform in OT. Two contributing factors cover the majority of the difficulties seen during OT:

- Network connectivity and congestion. Most DT labs use a hardwired network with unlimited bandwidth, but during OT the system uses a tactical network with limited bandwidth. The limitations can cause the network to time-out, resulting

in a system failure. DT labs should emulate the expected operational networks as accurately as possible and simulate tactical network bandwidth, connectivity, and congestion.
- Interfacing systems. Each of the interfacing systems may have peculiarities which are not well understood during DT. Operational interfaces may have software patches to compensate for problems experienced during operation and thus work differently from the initial design. These differences might be enough to cause the system under test to fail to support the user's mission. DT labs should have the latest versions of the key interfacing systems and use as much operationally realistic data as possible.

Persistent Maintenance of the Cybersecurity Plan of Actions and Milestones

An enterprise network requires MAIS programs to interface with multiple outside programs, which often include commercial systems. Allowing such connections is inherently risky from a cybersecurity perspective, and often makes it impossible to eliminate all vulnerabilities. Thus, it is important to identify, document, and continue to monitor those risks. A cybersecurity Plan of Actions and Milestones (POA&M) is the best tool to identify and document cybersecurity vulnerabilities and the mitigations for them. The POA&M should clearly identify all of the vulnerabilities by priority and urgency, the proposed corrective actions, responsible organization and person, and the milestone to achieve correction. It should include vulnerabilities associated with interfacing systems, and should not be a document that is approved once and put away; the threats are dynamic, as are the network environments.

Continual awareness of emerging cybersecurity threats, realistic adversarial testing of the system against those threats, and implementing mitigations for vulnerabilities should be an ongoing process supported by decision-makers with the authority to require corrective actions. With appropriate leadership's focus, MAIS programs with extensive cybersecurity vulnerabilities have successfully resolved them. For example, the Navy's Consolidated Afloat Networks and Enterprise Services (CANES) program had hundreds of significant cybersecurity vulnerabilities as it entered into IOT&E, but successfully tracked and fixed a sufficient number of them to be more secure against cyber-attacks. The CANES program will have to continue to maintain its POA&M to discover and fix cybersecurity vulnerabilities as the threats and the network continue to evolve.

Thorough Tracking of Software Problems in a Comprehensive Database and Senior-Level Review of Priorities

Agile development requires decision-makers to quickly modify the priority and urgency of functions from one release to another. For the decision-makers to make an informed decision on a short decision cycle, they need to understand the development status and challenges. Even within the release cycle, decision-makers may have to change the amount of resources devoted to a particular function. Therefore, the decision-makers need to know the number of open software problems by criticality and urgency, as well as the time and resources needed to resolve software deficiencies. If correcting a problem requires a long time and interferes with the fielding schedule, decision-makers should consider mission impact against the time and resources required to fix problems. This will help to decide whether to defer the delivery to the next release or rearrange resources to more quickly solve the problem. Both GCSS-A and LMP have good processes for senior-level Army leaders to review and prioritize fixes to software problems based on user input.

Implementing Best Practices through Agile Acquisition

The best practices identified in this report can help to improve the success of MAIS programs and should be applied broadly. In order to maximize the effectiveness of these practices, DOD should pursue the agile acquisition approach. Incremental software delivery is one aspect of agile acquisition and has already been implemented with some success. However, DOD can do more to accommodate agile software development. Using proven commercial agile frameworks is a good way to systematically integrate the best practices.

Incremental Software Delivery and Agile Acquisition

To overcome challenges associated with program complexity and requirements instability, DODI 5000.02 includes an acquisition model suitable for incremental software delivery.[6] Compared to a traditional "waterfall" model, where all of the functions are developed and delivered in one lengthy and monolithic acquisition cycle, incremental delivery allows each increment to focus on a selected set of functions, which reduces complexity. In addition, each increment takes a shorter time, and thus reduces the chance of requirement changes.

In a 2015 report, the GAO claimed:

> About half of the [selected 20 MAIS] programs that met or planned to meet this condition had been positioned to do so because they had been restructured and split into smaller, incremental programs, which is consistent with a Defense Science Board recommendation, Office of Management and Budget (OMB) guidance, and a statutory requirement to use incremental contracting to the maximum extent practicable for major IT acquisitions.[7]

However, working on multiple software releases, which often overlap, brings its own set of challenges – including difficult coordination among the key stakeholders and increases in redundancies and resource requirements. To help overcome these challenges, many MAIS programs adopted agile acquisition.

Agile acquisition (also known as agile software development) is an approach to software development that is built around a set of guiding principles established by the nonprofit Agile Alliance. This approach's practices and methods are in large part intended to improve efficiency, responsiveness to changing needs, and quality. Essential elements of agile acquisition include:
- Delivering working software quickly and improving/adapting it incrementally in frequent releases

---

6 DODI 5000.02, page 11, paragraph 5c(3)(d)
7 GAO report GAO-15-282, "Defense Major Automated Information Systems: Cost and Schedule Commitments Need to Be Established Earlier," February 26, 2015, page 15

- Collaborating directly with users
- Minimizing governance processes

Agile acquisition is only appropriate after the basic infrastructure is in place. While agile acquisition gives flexibility for adding or enhancing functions and applications, building a network infrastructure requires a deliberate and logically sequenced plan. For most DOD MAIS programs, network infrastructure is so complex and interrelated that there is not much flexibility, and this lack of flexibility nullifies the benefit of agile acquisition. A large system may have an infrastructure software component that is necessary for verification testing of other system components.[8] A program should have a working infrastructure that satisfies the Information Exchange Requirements and network protocol requirements, and have a sufficiently detailed architectural description to ensure each software module fits into the overall enterprise.

Additionally, a MITRE report advises:[9]

> … it is absolutely critical that the development of the architecture precede sprint development.[10] Alternatively, a program can initially use a traditional approach to build the initial increment that meets the baseline architecture requirements. Once the program has established the baseline and framed the overall conceptual design, program managers can consider shifting to an agile approach for subsequent increments that build additional functionality into the operational baseline.

For instance, DCGS-A and DCGS-Navy first delivered stable infrastructure with Increment 1, and are now moving to agile acquisition for Increment 2. In both cases, the first phases of Increment 2 improve data infrastructure before adding newer applications.

Implementing a Proven Agile Framework Product

Most successful commercial software developers use proven agile software development framework packages. Popular agile development framework products include Scrum, Extreme Programming, and Scaled Agile Framework (SAFe). These products systematically incorporate the best practices discussed in this section, and make it easy for MAIS programs to implement good ideas from both government and commercial developers. Scrum and SAFe are the approaches most often implemented by MAIS program managers.

The agile acquisition frameworks share common attributes: an integrated team approach that integrates users, developers, and testers; flexible management of requirements priority and urgency; small segments developed and tested before combining into larger segments; and many concurrent activities.

While the commercially available agile frameworks help build good acquisition structure, leaning how to use the frameworks is not easy. The program office needs to plan sufficient resources to train acquisition stakeholders. Air Force DCGS is starting to implement SAFe for its Open Architecture development and has heavily invested time and resources to train not only the program office, but everyone in the acquisition community – such as requirement owners, testers, and program sponsors. Such training is essential for the team approach; it is impossible to collaborate until everyone shares a common language and frame of reference.

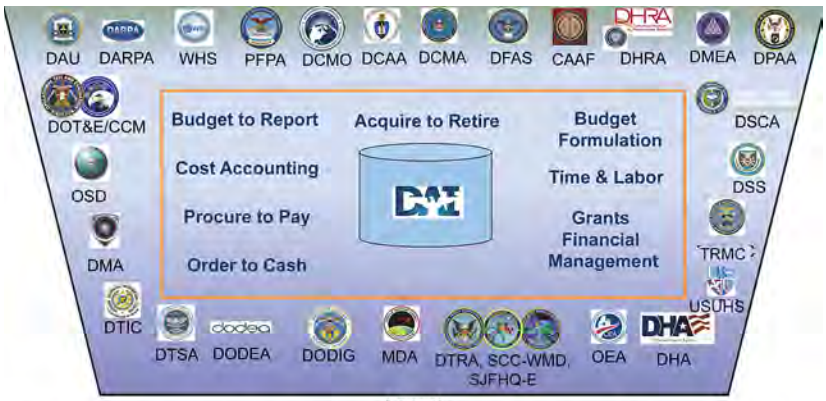
---

8 Carnegie Mellon University, Software Engineering Institute report, "Considerations for Using Agile in DoD Acquisition," 2010

9 The MITRE Corporation technical paper, "Defense Agile Acquisition Guide: Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities," March 2014

10 A "sprint" is a regular, repeatable work cycle in agile methodology during which work is completed and made ready for review.

Defense Agencies Initiative (DAI)



Legend

CAAF - Court of Appeals for the Armed Forces
DAI - Defense Agencies Initiative
DARPA - Defense Advanced Research Projects Agency
DAU - Defense Acquisition University
DCAA - Defense Contract Audit Agency
DCMA - Defense Contract Management Agency
DCMO - Deputy Chief Management Officer
DFAS - Defense Finance and Accounting Service
DHA - Defense Health Agency
DHRA - Defense Human Resources Activity
DMA - Defense Media Activity
DMEA - Defense Microelectronics Activity
DODEA - Department of Defense Education Activity
DODIG - Department of Defense Inspector General
DOT&E/CCM - Director, Operational Test & Evaluation including Center for Countermeasures (CCM)
DPAA - Defense Prisoner of War/Missing In Action Accounting Agency
DSCA - Defense Security Cooperation Agency
DSS - Defense Security Service
DTIC - Defense Technical Information Center
DTRA - Defense Threat Reduction Agency
DTSA - Defense Technology Security Administration
JSTO - Joint Science and Technology Office
MDA - Missile Defense Agency
OEA - Office of Economic Adjustment
OSD - Office of the Secretary of Defense
PFPA - Pentagon Force Protection Agency
SCC-WMD - US Strategic Command Center for Combatting Weapons of Mass Destruction
SJFHQ-E - Standing Joint Force Headquarters-Elimination
TRMC - Test Resource Management Center
USU - Uniformed Services University of the Health Sciences
WHS - Washington Headquraters Services

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) of the Defense Agencies Initiative (DAI) Increment 2 Release 2 from February 29 through March 18, 2016. During this OA, DAI successfully completed 98 percent of the users' critical tasks.
- During the OA, the DAI Program Management Office (PMO) provided data for only one of six high-level outcomes (HLOs) with defined measures.
- Both DAI's operational reliability and availability during the OA improved as compared to the previous OA; however, the system continues to require improvements in usability.
- During its cybersecurity testing, DAI was difficult to exploit by an outsider threat but was vulnerable to an insider threat with administrator credentials. Neither DAI nor the network defenders detected Red Team activity or an event designed to artificially stimulate a reaction.
- DAI's annual continuity of operations (COOP) exercise verified that the alternate site could restore partial mission or business processes, but hosting limitations prohibits the system from efficiently reconstituting back to the primary DAI site.

System

- DAI is an integrated financial management solution that provides a real-time, web-based system of integrated business processes and is used by defense agency financial managers, program managers, auditors, and the Defense Finance and Accounting Service (DFAS). DAI's core functionality is based on Oracle E-Business Suite Release 12.2.3 (a commercially available enterprise solutions system).
- DAI subsumes many systems and standardizes business processes for multiple DOD agencies and field activities. It modernizes the financial management processes by streamlining financial management capabilities, addressing financial reporting material weaknesses, and supporting financial statement auditability.
- The Defense Information Systems Agency (DISA) provides facilities, network infrastructure, and the hardware operating system for the DAI servers at its Ogden, Utah, and Columbus, Ohio, Defense Enterprise Computing Centers.
- DAI is employed worldwide and across a variety of operational environments via a web portal on the Non-secure Internet Protocol Routing Network (NIPRNET) using each agency's existing information system infrastructure.

- DAI includes two software increments:
  - Increment 2 replaces Increment 1 and is in use for financial reporting at 12 defense agencies.
  - Increment 2 has four software releases, each with additional capabilities, with deployments to 15 additional defense agencies continuing through FY17. With the completion of Release 2.2 fielding on June 20, 2016, DAI provides services to 20 defense agencies and field activities with 29,852 users at 856 locations worldwide.
- DAI supports financial management requirements in the Federal Financial Management Improvement Act and DOD Business Enterprise Architecture. Therefore, it is a key tool for helping the DOD to have its financial statements validated as ready for audit by the end of FY17 as required by the National Defense Authorization Act for FY10.

Mission

Financial Managers in defense agencies use DAI to transform their budget, finance, and accounting operations to achieve accurate and reliable financial information in support of financial accountability and decision making.

Major Contractors

- CACI Arlington – Arlington, Virginia
- International Business Machines – Armonk, New York
- Northrop Grumman – Falls Church, Virginia

Activity

- From November 16, 2015, to May 31, 2016, JITC and the DISA Risk Management Executive Red Team completed a Cooperative Vulnerability and Penetration Assessment, an Adversarial Assessment, and a Cyber Economic Vulnerability Assessment (CEVA) to test the cybersecurity of DAI.
- From February 29 through March 18, 2016, JITC conducted an OA of DAI Increment 2 Release 2, in accordance with a DOT&E-approved test plan. The test was adequate, except the CEVA data fraud analysis portion, which JITC deferred until the IOT&E.
- The DAI PMO conducted three developmental test events of DAI Increment 2 Release 3 throughout FY16: a development integration test from January 6 through July 28, 2016; a system integration test from June 20 through July 28, 2016; and a user acceptance test conducted from August 2 through September 8, 2016.
- In coordination with DISA, the DAI PMO conducted its annual COOP exercise from April 25 – 29, 2016. As the hosting agency for DAI, DISA provides a mix of tabletop and remote recovery and simulation exercises to meet the program's system requirements.
- On October 7, 2016, USD(AT&L) signed an Acquisition Decision Memorandum approving limited fielding of DAI Increment 2 Release 3 to current and additional defense agencies.
- On November 9, 2016, USD(AT&L) signed an Acquisition Decision Memorandum approving development of DAI Increment 2 Release 4 with current and additional defense agencies.
- JITC and the DAI PMO are coordinating for a full cybersecurity test (Cooperative Vulnerability and Penetration Assessment, Adversarial Assessment, CEVA, and COOP) for 2Q – 3QFY17 as part of the IOT&E on Increment 2 Release 3.

Assessment

- During the Release 2 OA, DAI successfully completed 669 of 682 critical tasks (98 percent). The 13 unsuccessful tasks include hardware, software, or system errors that have been corrected and user errors that better training and user documentation could address.
- Comparing DAI's performance during the Release 2 OA to the Release 1 OA, the mean time between system failure improved from 292 to 328 hours and operational availability improved from 83 to 89 percent. The DAI PMO more closely managed scheduled maintenance to increase reliability and availability to users worldwide.
- Users opened 13 critical-level problem tickets from November 1, 2015, to March 18, 2016, and the DAI PMO resolved all within 4 days. Users also opened 189 major-level problem tickets during the same timeframe; by May 10, 2016, the DAI PMO had resolved all but 5 of the tickets.
- The DAI Increment 2 Business Case defines the HLOs, which quantitatively establish the value added by DAI Increment 2. However, of the six HLOs with defined measures, JITC measured only "Automate Absence Management" during the Release 2 OA. During the IOT&E, the DAI PMO must provide data for the remaining HLOs in order to provide a detailed, realistic assessment of the effectiveness of the program.
- In spite of the improvements in the DAI system, users gave the program a System Usability Score of 48, down from 59 reported in the Release 1 OA. Factors causing that decline include:
  - There was a 15 percent increase in DAI users with less than 2 years of experience with the system. Those users scored DAI lower than users with more experience.
  - Frequent user comments on DAI functionality related to the slowness and difficulty to enter data and generate DAI reports, queries, and search requests.
- During the Adversarial Assessment, the DISA Red Team – using limited to moderate cyber-attack capabilities – was unable to exploit DAI as an outsider or as an insider with user-level credentials. However, as an insider with administrator-level access, the Red Team identified four vulnerabilities. Neither DAI nor the network defenders

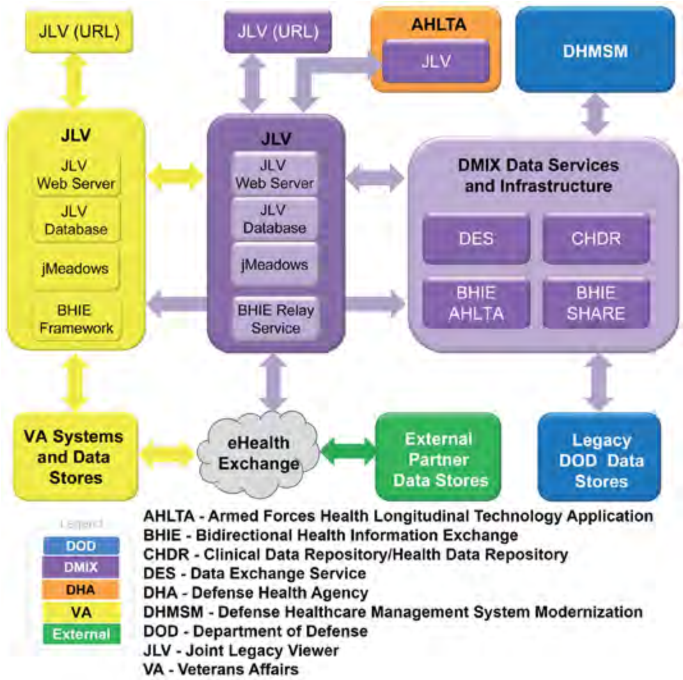
detected the Red Team or an event designed to artificially stimulate a reaction.

- During the CEVA, agencies' financial experts concluded that the existing technical checks would make it difficult to exploit known or potential vulnerabilities to commit fraud.
- During the COOP exercise, DAI PMO testers successfully executed selected business functions on alternate site servers, which verified that the alternate site could restore partial mission or business essential functionality. Because of the limited users and tasks, testing did not include load or performance testing. At present, DISA does not provide reconstitution (failover) as a service which precludes DAI from performing a full reconstitution exercise for the COOP environment.

Recommendations

- Status of Previous Recommendations. The program has implemented changes to address the FY15 recommendations, but the fraud analysis portion of the CEVA was deferred until the IOT&E.
- FY16 Recommendations. The DAI PMO should:
  1. Improve system performance to reduce response times and unexpected errors.
  2. Provide high-level outcome data to JITC both before and during the IOT&E for evaluation of operational effectiveness.
  3. Improve training and documentation to include error message handling, reports and queries in DAI or Oracle business intelligence, and other advanced training courses.
  4. Work with DISA to improve real-time cybersecurity detect and react capabilities for DAI and mitigate known vulnerabilities.
  5. Improve COOP site architecture and capabilities with a goal of developing a data replication capability from COOP to production site.

Defensive Medical Information Exchange (DMIX)



Executive Summary

Defense Medical Information Exchange Program

- The Program Executive Officer Defense Healthcare Management Systems (PEO DHMS) moved the Defense Medical Information Exchange (DMIX) program under the DOD Healthcare Management System Modernization (DHMSM) program in August 2016.
- PEO DHMS released a DMIX Full Deployment Decision Acquisition Decision Memorandum on October 12, 2016, officially transitioning DMIX into sustainment.

Defense Medical Information Exchange Release 3

- The U.S. Army Medical Department Board (USAMEDDBD) and Air Force Medical Information Systems Test Bed (AFMISTB) conducted the DMIX Release 3 (R3) Multi-Service Operational Test and Evaluation (MOT&E) at the Air Force Academy, Colorado Springs, Colorado; Fort Carson, Colorado Springs, Colorado; Joint Base Elmendorf-Richardson (JBER), Anchorage, Alaska; and Fort Drum, Watertown, New York, in April and May 2016. The DMIX R3 MOT&E was adequate to evaluate operational effectiveness and suitability. DOT&E did not assess survivability.
- DMIX R3 is operationally effective for queries of DOD and Department of Veterans Affairs (VA) data, but not for external healthcare partner data. Users were able to open all notes with the exception of two Community Health Summary (CHS) notes at JBER. All test patient data evaluated were accurate and timely. All DMIX R3 critical external interfaces met accuracy and timeliness threshold values. The majority of effectiveness failures that DOT&E observed during the test were attributable to two problems:
  - External partner data did not populate in the Immunizations widget.
  - The CHS widget did not consistently open for JBER users, preventing them from viewing external partner data.
- DMIX R3 is operationally suitable. Users rated DMIX R3 usability highly on the System Usability Scale (SUS) and indicated that the response time is adequate. Overall, DMIX R3 availability satisfied the threshold, with DMIX-owned components having higher availability than the required interfacing systems. Overall, 40 percent of the users felt they needed more training on the system.
- DOT&E did not assess DMIX R3 survivability. The cybersecurity Adversarial Assessment (AA) for DMIX R3 was delayed because of test limitations imposed by Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) Montgomery that did not allow for an adequate test. Cyber testers are planning to conduct a Cooperative Vulnerability and Penetration Assessment (CVPA) and AA on DMIX Release 5 in 1Q – 2QFY17.
- The DOD offered to include VA DMIX components and interfacing VA systems in the full-scope cybersecurity testing planned for DMIX R3, but the VA declined to participate. Instead, the VA requested that the Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services team conduct a limited-scope Risk and Vulnerability Assessment in April 2016. The scope of this assessment was not adequate to evaluate the full DMIX program, and did not include an AA, which is a critical part of DOT&E assessments of DOD systems. The DHS identified two critical vulnerabilities that could result in the loss of confidentiality, integrity, or availability of personal health information and personally identifiable information.

Defense Medical Information Exchange Releases 4 and 5

- The DMIX Program Manager developed and developmentally tested DMIX Releases 4 and 5 in 2016. PEO DHMS fielded DMIX Release 4 in July 2016 and DMIX Release 5 in October 2016.
- DOT&E agreed to allow PEO DHMS to include DMIX operational testing within the scope of the DHMSM IOT&E.

Terminology Mapping

- In late FY15 and FY16, the VA independently tested VA and DOD terminology maps to compare cross-organizational mapping and to inform efforts towards computable interoperability. The VA evaluated maps developed separately by the DOD and VA in five clinical domains. The testing evaluated the terminology within each map as well as the correlation between the two organizations' maps. The VA had not finalized results from this test in time to be included in this report.

System

- The DMIX program supports integrated sharing of standardized health data among DHMSM, DOD legacy systems, VA, other Federal agencies, and private-sector healthcare providers.
- Together, DHMSM and DMIX are intended to modernize the Military Health System to enhance sustainability, flexibility, and interoperability for improved continuity of care.
- The DOD is developing DMIX incrementally, delivering upgrades to already fielded capabilities:
  - The Joint Legacy Viewer (JLV) provides an integrated, read-only, chronological view of health data from DOD and VA electronic health record systems, eliminating the need for VA or DOD clinicians to access separate viewers to obtain real-time patient information. DOD and VA users logon to their respective JLV web servers using a URL address in their web browser. Users of the Armed Forces Health Longitudinal Technology Application can connect to the JLV web server through the system menu.
  - The Data Exchange Service (DES) receives user queries entered through JLV and queries DOD, VA, and external partner data stores, returning the results to jMeadows. jMeadows maps local VA and DOD clinical terms to standard medical terminology and aggregates the data for presentation by the JLV web server.
  - The Bidirectional Health Information Exchange (BHIE) enables the VA to access clinical data from multiple DOD and VA systems using the DES, BHIE Share, and Clinical Data Repository/Health Data Repository. The Clinical Data Repository/Health Data Repository enables bidirectional exchange of outpatient pharmacy and medication allergy data for checking drug-to-drug and drug-to-allergy interactions.

Mission

The DOD, VA, Federal agencies, and private-sector health providers use the DMIX infrastructure and services to:

- Share standardized health data using standard terminology
- Securely and reliably exchange standardized electronic health data with all partners
- Access a patient's medical history from a single platform, eliminating the need to access separate systems to obtain patient information
- Maintain continuity of care
- Exchange outpatient pharmacy and medication allergy data and check for drug-to-drug and drug-to-allergy interaction

Major Contractors

- Data Federation/JLV: Hawaii Resource Group – Honolulu, Hawaii
- Test Support: Deloitte – Falls Church, Virginia
- Program Manager support: Technatomy – Fairfax, Virginia

Activity

Defense Medical Information Exchange Program

- PEO DHMS moved the DMIX program under the DHMSM program in August 2016.
- PEO DHMS released a DMIX Full Deployment Decision Acquisition Decision Memorandum on October 12, 2016, officially transitioning DMIX into sustainment.

Defense Medical Information Exchange Release 3

- USAMEDDBD and AFMISTB conducted a DMIX R3 MOT&E in accordance with the DOT&E-approved test plan at the Air Force Academy, Colorado Springs, Colorado; Fort Carson, Colorado Springs, Colorado; Joint Base Elmendorf-Richardson, Anchorage, Alaska; and Fort Drum, Watertown, New York, in April and May 2016.
- The DHS conducted a Risk and Vulnerability Assessment of DMIX R3 components on VA networks in April 2016.

Defense Medical Information Exchange Release 4

- The DMIX Program Manager conducted developmental testing of DMIX Release 4 at Allegany Ballistics Laboratory, Rocket Center, West Virginia, from April 25 through June 24, 2016.
- The PEO DHMS conducted the DMIX Fielding Decision Review on July 14, 2016, and subsequently fielded DMIX Release 4.

Defense Medical Information Exchange Release 5

- The DMIX Program Manager conducted developmental testing of DMIX Release 5 at Allegany Ballistics Laboratory, Rocket Center, West Virginia, from August 19 through September 30, 2016.
- The PEO DHMS conducted the DMIX Fielding Decision Review on October 14, 2016, and subsequently fielded DMIX Release 5.

Terminology Mapping

- In late FY15 and FY16, the VA independently tested VA and DOD terminology maps in five clinical domains to compare cross-organizational mapping and to inform efforts towards computable interoperability.

Assessment

- DMIX R3 is operationally effective for queries of DOD and VA data, but not for external healthcare partner data. All test patient records displayed in JLV were accurate as compared to the source data. Test patient data displayed in JLV were complete in 97 percent of the queries. Failures resulting from external healthcare partner data not displaying in the Immunizations widget accounted for 16 of the 20 completeness failures. Users opened all widgets successfully 92 percent of the time. The majority of failures to open all widgets (57 of 64) were failures to open the CHS widget at JBER. Widget sets downloaded within the 2 minute threshold 90 percent of the time. Users had a success rate of 99 percent when opening a note. Of the successful note downloads by DOD users, all notes displayed within 60 seconds. All but 2 of the CHS notes successfully downloaded by VA users at JBER displayed within 60 seconds.
- The Joint Interoperability Test Command evaluated four critical external interfaces using jMeadows server log files provided by the program manager. All four – namely the Patient Discovery Web Services, Master Veteran Index, DES, and Veterans Health Information Systems and Technology Architecture Data Service – met accuracy and timeliness threshold values.
- DMIX R3 is operationally suitable. Users rated DMIX R3 usability highly, with a mean score of 80 on the SUS. There were no significant differences in SUS ratings between sites, agencies, or user experience with JLV. Users liked the JLV data display and indicated that the response time was adequate. They liked the help features with the exception of error messages; users documented 107 test incidents regarding unclear error messages that did not adequately support them. Overall, 40 percent of the users (71 of 178) felt they needed more training on the system. Users who reported receiving only computer-based training, which is the primary medium, most often felt that they needed more training. The DMIX help desk was responsive and resolved help desk tickets in a timely manner. DMIX R3 availability – i.e., the ability of any user to query the system via JLV at a given time and potentially to view a patient's entire record – was 92.5 percent. This measure included supporting systems but did not account for the availability of DOD or VA databases. DMIX system components showed availability of 99.7 percent for JLV/jMeadows and 98.3 percent for DES.
- DOT&E did not assess DMIX R3 survivability. The cybersecurity AA for DMIX R3 was delayed because of test limitations imposed by DISA DECC Montgomery that did not allow for an adequate test. Cyber testers are planning to conduct a CVPA and AA on DMIX Release 5 in 1Q – 2QFY17, while also working with DISA to mitigate prior test limitations.
- The DOD offered to include DMIX components and interfacing systems on VA networks in the full-scope cybersecurity testing planned for DMIX R3, but the VA declined to participate. Instead, the DHS National Cybersecurity Assessment and Technical Services team conducted a limited-scope Risk and Vulnerability Assessment at the request of the VA. Testing included vulnerability scanning as well as penetration testing of the VA JLV server stack. The scope of this assessment was not adequate to evaluate the full DMIX program because other DMIX components and interfacing systems were not included in the assessment. The VA did not conduct an AA, which is a critical part of DOT&E assessments of DOD systems. The DHS identified two critical vulnerabilities that could result in the loss of confidentiality, integrity, or availability of personal health information and personally identifiable information.

Defense Medical Information Exchange Releases 4 and 5

- The DMIX Program Manager developed and developmentally tested DMIX Releases 4 and 5 in 2016. PEO DHMS fielded DMIX Release 4 in July 2016 and DMIX Release 5 in October 2016.
- DOT&E agreed to allow PEO DHMS to include DMIX operational testing within the scope of the DHMSM IOT&E.

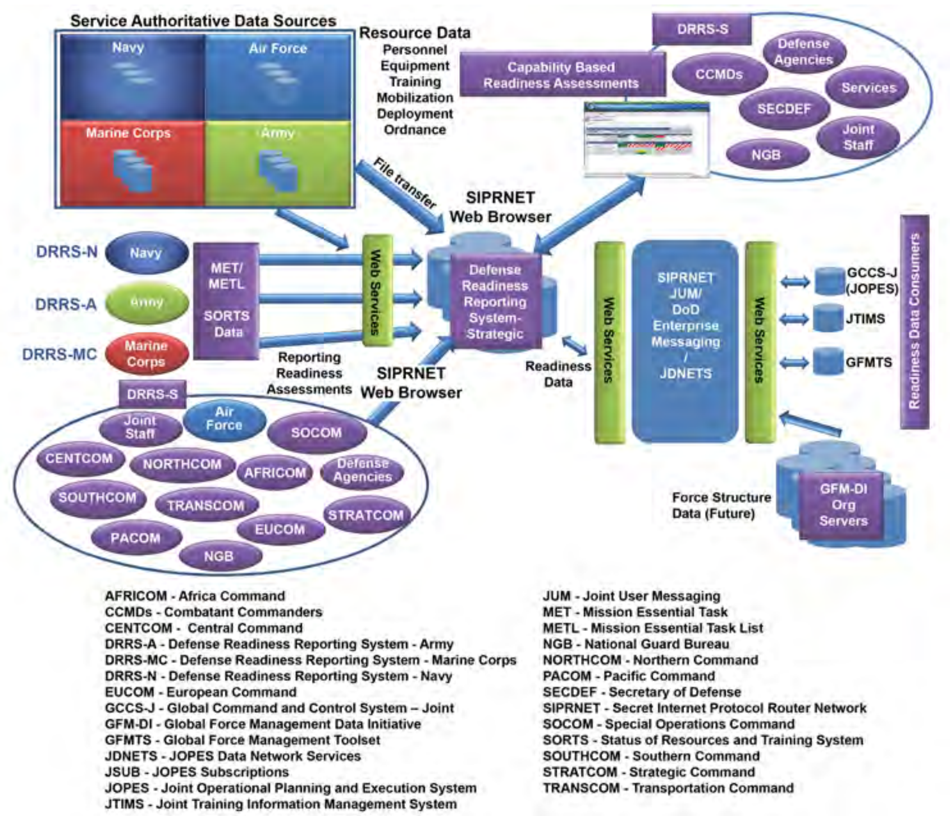
Terminology Mapping

- The VA independently evaluated the VA-DOD data maps for the Vital Signs, Medications, Payers, Documents, and Allergies clinical domains using a Structured Query Language analysis. This evaluation compared terminology within the maps individually as well as the correlation between the two organizations' maps. The VA had not finalized results from this test in time to be included in this report.

Recommendations

- Status of Previous Recommendations. The DMIX PMO has addressed the FY15 recommendations.
- FY16 Recommendations.
  1. The DMIX Program Manager should:
     - Diagnose and correct CHS problems.
     - Alert users when data do not load or are not available.
     - Improve error messages to provide users with better feedback where feasible.
     - Conduct DMIX Release 5 operational testing in conjunction with cybersecurity testing (CVPA and AA).
  2. The PEO DHMS should expand VA testing of correlation between the DOD and VA terminology maps to more clinical domains in order to fully understand the interoperability of medical records between the two organizations.
  3. The VA should:
     - Correct JLV cybersecurity vulnerabilities discovered during the DHS Risk and Vulnerability Assessment.
     - Allow a DOD Red Team to perform cybersecurity testing (CVPA and AA) of DMIX components and interfacing systems on VA networks.

Defense Readiness Reporting System – Strategic (DRRS-S)



Executive Summary

- The Joint Interoperability Test Command (JITC) conducted the Defense Readiness Reporting System – Strategic (DRRS-S) IOT&E from May 2015 through June 2015. Emerging results identified significant system and end-to-end process deficiencies. The DRRS-S Program Manager (PM) requested an extension of the IOT&E through October 2015 to correct system deficiencies and allow JITC to independently validate the fixes. DOT&E agreed to the extension. JITC continued IOT&E in September and October 2015. The IOT&E was adequate to evaluate operational effectiveness, suitability, and survivability.
- DRRS-S is operationally effective. Tactical units entered objective, accurate, and timely resources and training measurement data into DRRS-S and the Service DRRS variants to inform resource assessments of core missions and other mission assessments of units at all levels. The Service DRRS variants for the Army, Navy, and Marine Corps effectively published these data to DRRS-S, such that users could view all readiness assessments within DOD from the DRRS-S application.
- DRRS-S is operationally suitable. Users assessed the system usability as being acceptable. Users accessed the DRRS-S mission readiness view in a mean time of 20 seconds, well below the 5 minutes required. The system was operationally available 99.9 percent of the time and help desk support was responsive to user requests for assistance. Users reported no critical software failures between June and October 2015.
- DRRS-S is operationally survivable against a cyber threat with moderate capabilities. The DRRS PM corrected most cybersecurity vulnerabilities discovered in the Cooperative Vulnerability and Penetration Assessment phase of testing, and the Red Team could not exploit them during the Adversarial Assessment.
- Based upon the IOT&E Emerging Results Brief, dated February 17, 2016, the Principal Deputy Assistant Secretary of Defense (Readiness) and the Director of the Joint Staff approved the transition from the Global Status of Resources and Training System to DRRS-S on March 1, 2016.

System

- DRRS-S is a Secret Internet Protocol Router Network-accessible web application designed to replace the Global Status of Resources and Training System, a force readiness component of Global Command and Control System – Joint.
- DRRS-S production and backup systems are hosted at separate Defense Enterprise Computing Centers on commercial off-the-shelf hardware consisting of application and database server enclaves using Microsoft Windows operating systems.
- DRRS-S receives and processes readiness reports and data from Service-specific increments of the larger DRRS enterprise, including DRRS-Army, DRRS-Marine Corps, and DRRS-Navy. Combatant Commanders and the subordinates they direct, DOD agencies, and Air Force units report directly within DRRS-S.

Mission

- The Combatant Commanders, military Services, Joint Chiefs of Staff, Combat Support Agencies, and other key DOD users (such as the SECDEF and National Guard) use the DRRS collaborative environment to evaluate the readiness and capability of U.S. Armed Forces to carry out assigned and potential tasks.
- Reporting organizations input both mission readiness and unit readiness data – such as Status of Resources and Training System data – into DRRS-S and use it to make mission readiness assessments against standardized missions and tasks.

Major Contractor

InnovaSystems International, LLC – San Diego, California

Activity

- From May 2015 through June 2015, JITC conducted an IOT&E in accordance with the DOT&E-approved test plan. The IOT&E revealed a number of significant deficiencies with the system and end-to-end data management processes. Therefore, the DRRS-S PM requested an extension of the IOT&E through October 2015 to allow for the correction of system deficiencies and provide sufficient time for JITC to independently verify the fixes. DOT&E agreed to the extension.
- JITC continued the IOT&E in September and October 2015 using the DOT&E-approved test plan. This test window included two monthly readiness reporting cycles to verify the accuracy, completeness, and timeliness of Service readiness reports.
- JITC and the Army Research Laboratory, Survivability and Lethality Analysis Directorate, conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment from February 2015 through May 2015. The Defense Information Systems Agency Risk Management Executive Red Team conducted a cybersecurity Adversarial Assessment in June 2015.
- Based upon the IOT&E Emerging Results Brief, dated February 17, 2016, the Principal Deputy Assistant Secretary of Defense (Readiness) and the Director of the Joint Staff approved the transition from the Global Status of Resources and Training System to DRRS-S on March 1, 2016.

Assessment

- DRRS-S is operationally effective. Tactical units entered objective, accurate, and timely resources and training measurement data into DRRS-S and the Service DRRS variants to inform resource assessments of core missions and other mission assessments of units at all levels. The Service DRRS variants for the Army, Navy, and Marine Corps effectively published these data to DRRS-S, such that users could view all readiness assessments within DOD from the DRRS-S application. DRRS-S could then publish readiness assessment information to other critical downstream consumers, such as the Joint Operations Planning and Execution System and the Global Combat Support System (GCSS) – Joint. The Services' and the Joint Staff's readiness staffs faced some challenges to attain a common understanding of the current reporting status of all DOD units, but close coordination allowed staff members to explain apparent differences in readiness data. The Services' and Joint Staff's representatives agreed that the adverse mission impact of the apparent differences was low.
- The information in DRRS-S is only as objective, accurate, and timely as the data received and processed from the Services. DOT&E's evaluation of DRRS-S resource category levels considered whether they were consistent with 1) Service-reported resource levels, to assess DRRS-S accuracy and timeliness, and 2) the prescribed procedures in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.02B, to assess objectivity of DRRS-S data. As discussed above, DRRS-S data were accurate and timely.
  - Air Force assessments were consistent with CJCSI guidance for all four resource and training categories.
  - The Army's method for calculating the Equipment Condition/Readiness level (referenced as the R-level) relies on dated information from the Army Material Status System report, which provides availability rates from the previous month. The Army plans to follow the CJCSI rule more precisely after the maintenance functions in GCSS-Army are fielded in FY17. DOT&E expects that Army assessments will be consistent with CJCSI guidance once the Army fields GCSS-Army maintenance functions.
  - Marine Corps assessments were consistent with the CJCSI guidance with the observation that units must manually transcribe data from GCSS-Marine Corps into DRRS-Marine Corps, which increases workload and the chance for errors.

- Navy assessments were inconsistent with the CJCSI guidance, with only 30 percent (10 of 33) of assessed levels in DRRS-S consistent with the objective Figures of Merit in DRRS-Navy. The differences primarily are due to commander subjective upgrades of the readiness levels, which could reflect that the commander has more current knowledge than DRRS-S. However, some of the upgrades indicate some variation from the objective criteria in the CJCSI for the Navy core resource levels. The Navy should improve its guidance to commanders so that the DRRS-S resource levels are based on objective criteria, consistent with the Figures of Merit in DRRS-Navy.

- DRRS-S is operationally suitable. Users assessed the system usability as being acceptable, as evidenced by the average System Usability Scale score of 70.9, a high score for a DOD system. Users accessed the DRRS-S readiness view in a mean time of 20 seconds, well below the 5 minutes required. The system was operationally available 99.9 percent of the time and help desk support was responsive to user requests for assistance. Users reported no critical software failures between June and October 2015. A third of users responding in the survey felt that they needed more training, especially on the Air Force Input Tool, and this is substantiated by help desk requests for Business Intelligence Tool access and training. Although the DRRS PM has procedures to inform the Services whether published messages were processed, users still observed data mismatches between the Service DRRS variants and DRRS-S, such as duplicate or out-of-date mission assessments. The Joint Staff and Services should improve existing policies and procedures to verify currency of data and to correct data mismatches between DRRS-S and the Service DRRS variants.
- DRRS-S is operationally survivable against a cyber threat with moderate capabilities. The DRRS PM corrected most cybersecurity vulnerabilities discovered in the Cooperative Vulnerability and Penetration Assessment phase of testing, and the Red Team could not exploit them during the Adversarial Assessment.

Recommendations

- Status of Previous Recommendations. The DRRS-S Program Office addressed all previous recommendations.
- FY16 Recommendations.
  1. The Joint Staff, Services, and DRRS PM should establish policy and procedures to periodically review reporting units in DRRS against the Service and Joint Staff sources for currency and accuracy. The DRRS PM should assess duplicate or out-of-date mission-essential tasks in DRRS-S and coordinate with the Services and Joint Staff to correct the data on a regular basis.
  2. The DRRS PM should improve training related to DRRS-S features, including business intelligence and quick search tools.
  3. The Air Force should provide additional training to Air Force Input Tool users.
  4. The DRRS PM should mitigate the vulnerabilities reported in the cybersecurity tests and conduct follow-on evaluations of cybersecurity.
  5. The Navy should review its policy and procedures for determining the measured resource levels to reduce the need for commander upgrades. The Navy should also provide guidance to commanders for relating the objective Mission Area Figure of Merit scores and measurement data, if current, to more objective Personnel (P), the equipment Readiness/serviceability (R), Supply/equipment on hand (S), and Training (T) (PRST) ratings.
  6. The Army should base the R-level calculation on equipment Readiness/serviceability using GCSS-Army readiness data when the system is fully fielded.
  7. The Marine Corps should work to keep logistics transactions current at the GCSS-Marine Corps hub. The Marine Corps should also auto-populate GCSS-Marine Corps business intelligence authoritative data into the DRRS-Marine Corps to assist units in data entry.

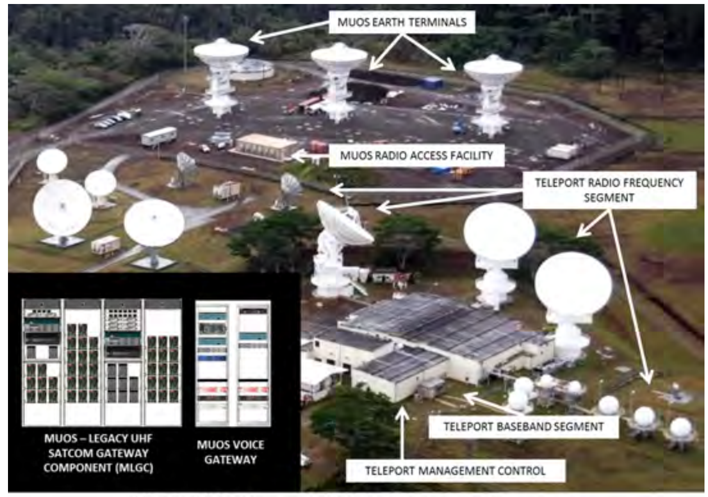
Department of Defense (DOD) Teleport

Executive Summary

- The Defense Information Systems Agency (DISA) is developing the Teleport Generation 3 Phase 3 (G3P3) capability that is intended to provide interconnectivity between legacy Ultra High Frequency (UHF) radios and Mobile User Objective System (MUOS) radios. To achieve the G3P3 capability, the program manager is adding two new components to the Teleport architecture: the MUOS to Legacy Gateway Component (MLGC) and MUOS Voice Gateway (MVG). The program manager is planning to install the MLGC at five of the six primary Teleport sites and the MVG at the Virginia and Hawaii Teleport sites, collocated with two MUOS Radio Access Facilities.
- During developmental test and evaluation (DT&E), DISA tested G3P3 voice capability but did not test data capability. The unclassified voice test results met the 88 percent required completion rate, but classified legacy to MUOS voice did not meet this completion rate. The data DISA collected during DT&E were insufficient to provide statistical confidence.
- DISA postponed the OT&E from October 2016 to 4QFY17, and the FOT&E from 4QFY17 to 1QFY18 due to technical and integration problems. The program manager is conducting root cause analysis and corrective actions to address the problems.

System

- DOD Teleport sites are globally distributed Satellite Communication (SATCOM) facilities. There are six core Teleport facilities located in Virginia, Germany, Italy, Japan, Hawaii, and California, and two secondary facilities located in Bahrain and Australia (future). Teleport sites consist of four segments:
  - The radio frequency segment consists of SATCOM earth terminals that operate in UHF, X, C, Ku, Ka, and Extremely High Frequency bands. The terminals provide radio frequency links between the Teleport site and the deployed user SATCOM terminal via military or commercial satellites.
  - The baseband segment includes encryption, switching, multiplexing, and routing functions for connecting data streams or packetized data to the terrestrial Defense Information Systems Network (DISN).



MLGC - MUOS-Legacy UHF STACOM Gateway Component
MUOS - Mobile User Objective System
UHF - Ultra High Frequency

  - The network services segment provides connectivity to the DISN long-haul networks and other internet functions necessary to meet the user's requirements.
  - The management control segment provides centralized monitoring and control of Teleport baseband hardware, earth terminal hardware, transmission security, and test equipment.
- Teleport provides deployed forces access to standard fixed gateways from anywhere in the world for all six DISN services:
  - Secret Internet Protocol Router Network
  - Non-secure Internet Protocol Router Network
  - Defense Red Switch Network
  - Defense Switched Network
  - Video Teleconference
  - Joint Worldwide Intelligence Communications System

Mission

Combatant Commanders, Services, and deployed operational forces use DOD Teleport systems in all phases of conflict to gain access to worldwide military and commercial SATCOM services.

Major Contractor

Government Integrator: DISA – Fort Meade, Maryland

Activity

- DISA is developing the Teleport G3P3 capability that is intended to provide interconnectivity between legacy UHF radios and MUOS radios. To achieve the capability, the program manager is adding two new components to the Teleport architecture, the MLGC and MVG. The program manager is planning to install the MLGC at five of the six primary Teleport sites and the MVG at the Virginia and Hawaii Teleport sites, collocated with two MUOS Radio Access Facilities.

- DISA conducted the initial DT&E from April through May 2016 at the Northwest Teleport site in Chesapeake, Virginia. Deployed users participated from the Navy's USS *Gridley* (San Diego, California) and USS *Schamal* (Mayport, Florida); the Coast Guard's USCGC *Sherman* (Pearl Harbor, Hawaii); Air Station Elizabeth City, North Carolina; and the Army's 10th Mountain Division (Fort Drum, New York). Government technicians operated the MLGC at the Northwest Teleport, and operated radios at the Space and Naval Warfare Systems Command (SPAWAR) Systems Center in Charleston, South Carolina.
- DISA conducted DT&E-2 from July through August 2016 at the Northwest Teleport site. Deployed users participated from the Navy's USS *Sampson* (San Diego, California), the Army's 3rd Corps at Fort Hood, Texas, and the Air Force's 59th Test and Evaluation Squadron at Nellis AFB, Nevada. Government technicians operated the MLGC at the Northwest Teleport, and radios at the SPAWAR Systems Center in Charleston, South Carolina.
- DISA postponed the OT&E from October 2016 to 4QFY17, and the FOT&E from 4QFY17 to 1QFY18 due to technical and integration problems. The program manager is conducting root cause analysis and corrective actions to address the problems.
- The Joint Interoperability Test Command is developing the operational test plan, with guidance from DOT&E.

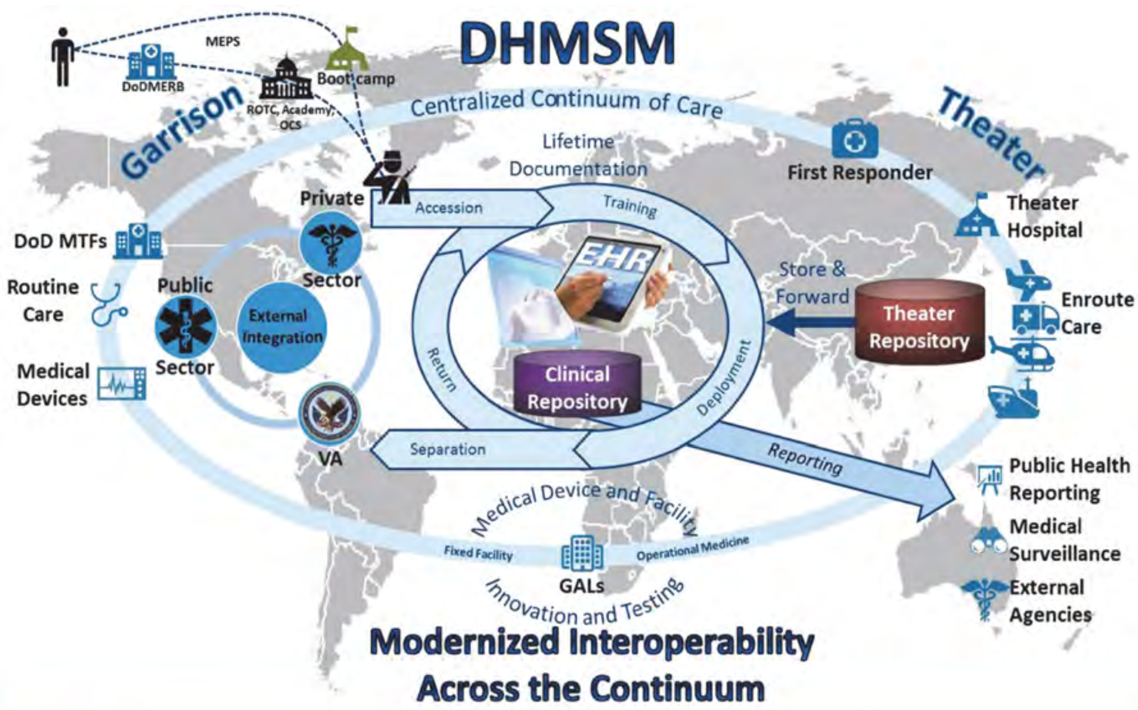
Assessment

- Since the Services have not yet fielded MUOS terminals, operator inexperience and immature user operations impaired effective involvement of deployed users for testing. Inexperience contributed to problematic cryptographic key management, problems creating profiles for the MUOS terminal, and the inability of a MUOS terminal to join an Internet Protocol network. User experience and proficiency will be essential to successful future operational testing.
- During DT&E, DISA tested the G3P3 voice capability but did not test the data capability. The unclassified voice test results met the 88 percent required completion rate but classified legacy-to-MUOS voice did not meet this completion rate. The data DISA collected during DT&E were insufficient to provide statistical confidence.
- During DT&E-2, DISA tested both G3P3 classified and unclassified voice and unclassified data capabilities. The classified legacy UHF to MUOS voice test results indicate that the capability may not be operationally viable without changes to techniques and procedures. The data DISA collected during the DT&E-2 were insufficient to provide statistical confidence.

Recommendations

- Status of Previous Recommendations. DISA has satisfactorily addressed all previous recommendations.
- FY16 Recommendation.
  1. The Joint Interoperability Test Command should ensure the data collected during the OT&E are sufficient to provide statistical confidence in the results.

DOD Healthcare Management System Modernization (DHMSM)



LEGEND:			
DHMSM	DoD Healthcare Management Systems Modernization	MERB	Medical Examination Review Board
DoD	Department of Defense	MTF	Military Treatment Facility
EHR	Electronic Health Record	OCS	Officer Candidate School
GAL	Government Authorized Laboratory	ROTC	Reserve Officers' Training Corps
MEPS	Military Entrance Processing Station	VA	Veterans Affairs

Executive Summary

- The Leidos Partnership for Defense Health (LPDH) began functional Contractor Integration Testing (CIT) of Military Health System (MHS) GENESIS at Leidos in Vienna, Virginia, on July 25, 2016. Over the succeeding 3 months, LPDH experienced a higher rate of functional and interface defects than expected.
- As of November 8, 2016, LPDH had successfully completed 70 percent (1,008 of 1,437) of the CIT test cases with 4 open Severity 1 and 75 open Severity 2 defects. At that time, LPDH had fixed and successfully retested 42 Severity 1 and 352 Severity 2 defects. A Severity 1 defect prevents the accomplishment of an essential capability and a Severity 2 defect adversely affects the accomplishment of an essential capability with no known workaround.
- Interface development has proved difficult for LPDH and legacy system owners, with the highest defect rates in the MHS GENESIS interfaces with the Defense Enrollment Eligibility Reporting System (DEERS) and Defense Medical Information Exchange (DMIX) system. Both of these interfaces are critical for MHS GENESIS to function correctly.
- The Defense Health Agency (DHA) Cybersecurity Division conducted a Risk Assessment of commercial services shared with the DOD at the Cerner Technology Center in Kansas City, Missouri, identifying over 8,000 cybersecurity vulnerabilities of varying severity. LPDH committed to have all mitigations for the highest severity vulnerabilities completed by December 31, 2016.
- The DHA Cybersecurity Division conducted an Independent Verification and Validation of DOD Specific Infrastructure at the Cerner Technology Center – Kansas City, identifying over 3,000 cybersecurity vulnerabilities of varying severity. The number of vulnerabilities identified by the DHA during the Risk Assessment and Independent Verification and Validation was larger than the program manager and LPDH expected.
- On October 7, 2016, USD(AT&L) approved a modified MHS GENESIS program schedule to allow the program manager additional time to finalize system interfaces, implement clinical capabilities, complete cybersecurity risk management, and provide time to test these capabilities prior to initial deployment. The new schedule delays go-live by 2 months, to

February 7, 2017, and changes the initial fielding site from the Naval Hospital Oak Harbor, Washington, to the 92nd Medical Group at Fairchild AFB, Washington. The program manager plans to go live at Naval Hospital Oak Harbor, Washington in May 2017, Naval Hospital Bremerton, Washington in June 2017, and Madigan Army Medical Center, Washington, in July 2017.
- Although the modified program schedule removes most of the overlap in testing, significant technical and schedule risks remain due to the large number of high severity defects and cybersecurity vulnerabilities that the program manager still needs to address.

System
- The DOD Healthcare Management System Modernization (DHMSM) program will acquire and field MHS GENESIS, a modernized Electronic Health Records (EHR) System, to 153,000 Military Health System personnel, providing care for 9.4 million DOD beneficiaries worldwide.
- MHS GENESIS comprises three major elements: 1) the Millennium suite of applications, developed by Cerner, which provides clinical capabilities; 2) Dentrix Enterprise, developed by Henry Schein Inc., which provides dental capabilities; and 3) Orion Rhapsody, the framework that enables the majority of the external information exchanges.
- The DHMSM program established two program segments to support deployment of the DHMSM EHR System to the DOD enterprise:
  - Fixed Facility (Segment 1) supports all medical and dental services delivered by permanent inpatient hospitals and medical centers, ambulatory care clinics, and dental clinics.
  - Operational Medicine (Segment 2) supports theater hospitals, hospital ships, forward resuscitative sites, naval surface ships, and submarines. The EHR System will be configured to work on the Operational Medicine infrastructure. The DHMSM program will provide MHS GENESIS to the Joint Operational Medicine Information System Program Office for implementation.
- DHMSM is intended to transition the DOD to a state-of-the-market EHR. It will replace legacy healthcare systems including the Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), and Essentris inpatient system. DHMSM will replace legacy Operational Medicine components of the Theater Medical Information Program – Joint software suite including AHLTA-Theater, TMIP CHCS Caché, and AHLTA-Mobile.

Mission

DOD medical staff will use the EHR to deliver enroute care, dentistry, emergency department, health, immunization, laboratory, radiology, operating room, pharmacy, vision, audiology, and inpatient/outpatient services. DOD medical staff will also use the EHR to perform administrative support, front desk operations, logistics, and business intelligence.

Major Contractors
- Leidos – Reston, Virginia
- Cerner – Kansas City, Missouri
- Accenture Federal Services – Arlington, Virginia
- Henry Schein Inc. – Melville, New York

Activity
- On July 25, 2016, the LPDH began functional CIT for DHMSM at Leidos in Vienna, Virginia.
- From July 18 – 29, 2016, the DHA Cybersecurity Division conducted a Risk Assessment of shared commercial services at the Cerner Technology Center – Kansas City.
- From August 1 – 12, 2016, the DHA Cybersecurity Division conducted an Independent Verification and Validation on DOD-specific infrastructure at the Cerner Technology Center – Kansas City.
- On August 15, 2016, the DHA provided Program Executive Officer, Defense Healthcare Management Systems (PEO DHMS) a list of MHS GENESIS minimum essential capability showstoppers that must be resolved prior to go-live at the IOC sites.
- On September 1, 2016, PEO DHMS announced that the DHMSM program schedule would be modified.
- On October 7, 2016 the Program Manager presented LPDH's plan to adjudicate, retest, and close all high severity defects to USD(AT&L), who subsequently approved a modified program schedule for MHS GENESIS. The new schedule delays go-live by 2 months, to February 7, 2017, and changes the initial fielding site from the Naval Hospital Oak Harbor, Washington to the 92nd Medical Group at Fairchild AFB, Washington.
- On October 24, 2016 the PEO DHMS provided the go-live dates for the remaining Initial Operational Capability (IOC) sites – Naval Hospital Oak Harbor, Washington in May 2017, Naval Hospital Bremerton, Washington in June 2017, and Madigan Army Medical Center, Washington in July 2017.
- On November 10, 2016 the program manager waived the Government Developmental Test (DT) entrance criteria and began the testing on November 14, 2016.
- The Joint Interoperability Test Command (JITC) is scheduled to conduct a scenario-based operational assessment (OA) with a Cooperative Vulnerability and Penetration Assessment (CVPA) in the Fixed Facility (FF) Government Approved Laboratory (GAL), Auburn, Washington, from February 13 through March 20, 2017.
- JITC plans to conduct IOT&E and a cybersecurity Adversarial Assessment in July and August 2017.

Assessment

- LPDH began functional CIT of MHS GENESIS at Leidos in Vienna, Virginia, on July 25, 2016. Over the succeeding 3 months, LPDH experienced a higher rate of functional and interface defects than expected, slowing CIT test case execution.
- Interface development has proved difficult for LPDH and legacy system owners, with the highest defect rates in the MHS GENESIS interfaces with the DEERS and DMIX system. The program manager and LPDH are reviewing terminology mapping disparities discovered between legacy systems and MHS GENESIS, to determine if changes are required to the DMIX terminology mapping tables or in MHS GENESIS.
- The DHA Cybersecurity Division Risk Assessment identified 3,606 Category (CAT) I, 4,185 CAT II, and 626 CAT III vulnerabilities. The CAT I, II, and III codes rate the severity of vulnerabilities, with CAT I vulnerabilities being the most severe. Exploitation of a CAT I vulnerability directly leads to loss of confidentiality, availability, or integrity of data. LPDH committed to have all mitigations for the highest severity vulnerabilities completed by December 31, 2016.
- The DHA Cybersecurity Division Independent Verification and Validation of DOD-specific infrastructure identified 397 CAT I, 2,764 CAT II, and 328 CAT III vulnerabilities. The majority of these vulnerabilities were related to commercial software patches not installed on assessed assets. The number of vulnerabilities identified by the DHA during the Risk Assessment and Independent Verification and Validation was larger than the program manager and LPDH expected. The program manager developed a Plan of Action and Milestones with mitigations to address the highest severity findings.
- The program manager provided the functional and test communities' full access to CIT testing and has been receptive to members' concerns and advice.
- The modified MHS GENESIS program schedule allows the program manager additional time to finalize system interfaces, implement clinical capabilities, complete cybersecurity risk management, and provide time to test these capabilities prior to initial deployment. Although the modified program schedule removes most of the overlap in testing, significant technical and schedule risks remain.
  - The number of open high severity defects discovered by LPDH during the CIT peaked at 15 Severity 1 and 148 Severity 2 defects on October 18, 2016. As of November 8, 2016, LPDH was working to close 4 Severity 1 and 75 Severity 2 defects and already had fixed and successfully retested 42 Severity 1 and 352 Severity 2 defects. A Severity 1 defect prevents the accomplishment of an essential capability and a Severity 2 defect adversely affects the accomplishment of an essential capability with no known workaround.
  - As of November 8, 2016, LPDH had successfully completed 70 percent (1,008 of 1,437) of planned CIT test. The program manager deferred or deleted 381 CIT test cases, reducing the total number planned from 1,818 to 1,437. LPDH is scheduled to complete CIT on November 25, 2016.
  - On November 10, 2016, the program manager waived the DT entrance criteria and began the testing on November 14, 2016. DOT&E advised the program manager against entering DT because he may need to devote time during DT to resolve incomplete interfaces, cybersecurity vulnerabilities, open defects, and previously untested functionality. If the program manager experiences high defect discovery rates in DT like LPDH experienced in CIT, there will be insufficient time to ensure the system works prior to go-live on February 7, 2017.
  - LPDH is scheduled to conduct two scenario-based integration and validation events in January 2017 to prepare the 92nd Medical Group for go-live at Fairchild AFB, Washington. JITC is scheduled to observe the integration and validation events and provide an independent observation memorandum to inform the go-live decision. The 92nd Medical Group go-live decision will be informed by developmental test results and integration and validation event observations, as no operational testing is scheduled prior to this decision date.
  - After go-live, LPDH will be maintaining two separate baselines, an operational MHS GENESIS baseline to support live operations and a test baseline to support the OA and future development. Because the system will go-live one week prior to the JITC-lead OA, the baselines will likely not be frozen to allow LPDH to correct deficiencies that may be discovered by the 92nd Medical Group.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The program manager should:
  1. Ensure all high-severity defects are mitigated prior to go-live at Fairchild AFB and all workarounds are documented and available to operational users.
  2. Validate that high severity cyber vulnerabilities identified during the DHA Risk Assessment and Independent Verification and Validation have been fixed or mitigated prior to go-live at Fairchild AFB.

F-35 Joint Strike Fighter

Executive Summary

Test Strategy, Planning, Activity, and Assessment

- The Joint Strike Fighter (JSF) Program Office (JPO) acknowledged in 2016 that schedule pressure exists for completing System Development and Demonstration (SDD) and starting Initial Operational Test and Evaluation (IOT&E) by August 2017, the planned date in JPO's Integrated Master Schedule. In an effort to stay on schedule, JPO plans to reduce or truncate planned developmental testing (DT) in an effort to minimize delays and close out SDD as soon as possible. However, even with this risky, schedule-driven approach, multiple problems and delays make it clear that the program will not be able to start IOT&E with full combat capability until late CY18 or early CY19, at the soonest. These problems include:
  - Continued schedule delays in completing Block 3F mission systems development and flight testing, which DOT&E estimates will likely complete in July 2018
  - Delayed and incomplete Block 3F DT Weapons Delivery Accuracy (WDA) events and ongoing weapons integration issues
  - Continued delays in completing flight sciences test points, particularly those needed to clear the full F-35B Block 3F flight envelope, resulting in a phased release of Block 3F envelope across the variants, with the full Block 3F envelope for F-35B not being released until mid-CY18
  - Further delays in completing gun testing for all three variants and recently discovered gunsight deficiencies
  - Late availability of verified, validated and tested Block 3F Mission Data Loads (MDLs) for planned IOT&E and aircraft delivery dates; DOT&E estimates the first validated MDLs will not be available until June 2018
  - Continued shortfalls and delays with the Autonomic Logistics Information System (ALIS) and late delivery of ALIS version 3.0, the final planned version for SDD, at risk of slipping from early CY18 into mid-CY18
  - Significant, well-documented deficiencies; for hundreds of these, the program has no plan to adequately fix and verify with flight test within SDD; although it is common for programs to have unresolved deficiencies after development, the program must assess and mitigate the cumulative effects of these remaining deficiencies on F-35 effectiveness and suitability prior to finalizing and fielding Block 3F
  - Overall ineffective operational performance with multiple key Block 3F capabilities delivered to date, relative to planned IOT&E scenarios which are based on various fielded threat laydowns
  - Continued low aircraft availability and no indications of significant improvement, especially for the early production lot IOT&E aircraft

  - Insufficient progress in verification of Joint Technical Data, particularly those for troubleshooting aircraft fault codes and for support equipment
  - Delays in completing the required extensive and time-consuming modifications to the fleet of operational test aircraft which, if not mitigated with an executable plan and contract, could significantly delay the start of IOT&E
  - Insufficient progress in the following areas which are required for IOT&E:
    - Development, integration, and testing of the Air-to-Air Range Infrastructure instrumentation into the F-35 aircraft
    - Flight testing to certify the Data Acquisition, Recording, and Telemetry pod throughout the full flight envelope
    - Development of other models, including the Fusion Simulation Model, Virtual Threat Insertion table, and the Logistics Composite Model
  - Delays in providing training simulators in the Block 3F configuration to the initial training centers and operational locations
- Based on these ongoing problems and delays, and including the required time for IOT&E spin-up, the program will not be ready to start IOT&E until late CY18, at the soonest, or more likely early CY19. In fact, IOT&E could be delayed to as late as CY20, depending on the completion of required modifications to the IOT&E aircraft.

Progress in Developmental Testing

- Mission Systems Testing
  - The program continues to pursue a cost- and schedule-driven plan to delete planned mission systems DT points by using other test data for meeting test point objectives in order to accelerate SDD close-out. This plan, if not properly executed with applicable data,

sufficient analytical rigor and statistical confidence, would shift significant risk to operational test (OT), Follow-on Modernization (FoM) and the warfighter.

- This risky approach would also discard carefully planned build-up test content in the Test and Evaluation Master Plan (TEMP) and the Block 3F Joint Test Plan (JTP), content the program fully agreed was required when those documents were signed. The program plans to "quarantine" JTP build-up test points, which are planned to be flown by the test centers, and instead skip ahead to complex graduation-level Mission Effectiveness Risk Reduction test points, recently devised to quickly sample full Block 3F performance. Then, if any of the Block 3F functionality appears to work correctly during the complex test points, the program would delete the applicable underlying build-up test points for those capabilities and designate them as "no longer required." However, the program must ensure the substitute data are applicable and provide sufficient statistical confidence that the test point objectives had been met prior to deleting any underlying build-up test points. While this approach may provide a quick sampling assessment of Block 3F capabilities, there are substantial risks. The multiple recent software versions for flight test may prevent the program from using data from older versions of software to count for baseline test point deletions because it may no longer be representative of Block 3F. The limited availability and high cost of Western Test Range periods, combined with high re-fly rates for test missions completed on the range, make it difficult for the program to efficiently conduct this testing. Finally, the most complex capabilities in Block 3F have only recently reached the level of maturity to allow them to be tested, and they are also some of the most difficult test points to execute (i.e., full Block 3F capabilities and flight envelope).
- Historical experience indicates this approach, if not properly executed, may delay problem discoveries and increase the risk to completing SDD and increase the risk of failure in IOT&E (as well as, much more importantly, in combat). In fact, the program needs to allocate additional test points – which are not in its current plans – for characterization, root cause investigations, and correction of a large number of the open high-priority deficiencies and technical debt described later in this report. The completion of the planned baseline test points from the Block 3F JTP, along with correction or mitigation of significant deficiencies, is necessary to ensure full Block 3F capabilities are adequately tested and verified before IOT&E and, more importantly, before they are fielded for use in combat.
- Until recently, the Program Office estimated that mission systems flight testing will complete in October 2017. It now acknowledges the risk that this testing may extend into early CY18.
  - The October 2017 estimate was based on an inflated test point accomplishment rate and optimistically low regression and re-fly rates. The estimate also assumed that the Block 3FR6 software, delivered to flight test in December 2016, would have the maturity necessary to complete the remaining test points and meet specification requirements without requiring additional versions of software to address shortfalls in capability. However, this is highly unlikely, since several essential capabilities – including aimed gunshots and Air-to-Air Range Infrastructure – had not yet been flight tested or did not yet work properly when Block 3FR6 was released.
  - The Services have designated 276 deficiencies in combat performance as "critical to correct" in Block 3F, but less than half of the critical deficiencies were addressed with attempted corrections in 3FR6.
  - Independent estimates from other Pentagon staff agencies vary from March 2018 to July 2018 to complete mission systems testing – all based on the current number of test points remaining and actual historic regression and re-fly rates from the flight test program. Even these estimates are optimistic in that they account for only currently planned testing, which does not yet include the activities needed to correct the Services' remaining high-priority deficiencies.

- Flight sciences testing continues to be a source of significant discovery, another indication that the program is not nearing completion of development and readiness for IOT&E. For example:
  - Fatigue and migration of the attachment bushing in the joint between the vertical tail and the aircraft structure are occurring much earlier than planned in both the F-35A and F-35B, even with a newly designed joint developed to address shortfalls in the original design.
  - Excessive and premature wear on the hook point of the arresting gear on the F-35A, occuring as soon as after only one use, has caused the program to consider developing a more robust redesign.
  - Higher than predicted air flow temperatures were measured in the engine nacelle bay during flight testing in portions of the flight envelope under high dynamic pressure on both the F-35A and F-35C; thermal stress analyses are required to determine if airspeed restrictions will be needed in this portion of the flight envelope.
  - Overheating of the horizontal tail continued to cause damage, as was experienced on BF-3, one of the F-35B flight sciences test aircraft, while accelerating in afterburner to Mach 1.5 for a loads test point. The left horizontal inboard fairing surface reached temperatures that exceeded the design limit by a significant amount. Post-flight inspections revealed de-bonding due to heat damage on the trailing edge of the horizontal tail surface and on the horizontal tail rear spar.
  - Vertical oscillations during F-35C catapult launches were reported by pilots as excessive, violent, and therefore a safety concern during this critical phase of flight. The program is still investigating alternatives to address this

deficiency, which makes a solution in time for IOT&E and Navy fielding unlikely.

Mission Data Load Development and Testing

- Mission data files, which comprise MDLs, are essential to enable F-35 mission systems to function properly. Block 3F upgrades to the U.S. Reprogramming Laboratory (USRL) – where mission data files are developed, tested and validated for operational use – are late to meet the needs for Block 3F production aircraft and IOT&E. These upgrades to the Block 3F configuration, including the associated mission data file generation tools, are necessary to enable the USRL to begin Block 3F mission data file development. In spite of the importance of the mission data to both IOT&E and to combat, the Program Office and Lockheed Martin have failed to manage, contract, and deliver the necessary USRL upgrades to the point that fully validated Block 3F MDLs will not be ready for IOT&E until June 2018, at the earliest.
- Operational units are also affected by the capability shortfalls in the USRL to create, test and field MDLs. The complete set of Block 2B and Block 3i MDLs developed for overseas areas of responsibility (AORs) have yet to undergo the full set of lab and flight tests necessary to validate and verify these MDLs for operational use. Because of the delays in upgrading the USRL to the Block 3F configuration, the Services will likely not have Block 3F MDLs for overseas AORs until late 2018 or early 2019.
- In addition to the late Block 3F USRL upgrades, the required signal generators for the USRL – with more high-fidelity channels to simulate modern fielded threats – have not yet been placed on contract. As a result, the Block 3F MDLs will not be tested and optimized to ensure the F-35 will be capable of detecting, locating, and identifying modern fielded threats until 2020, per a recent program schedule. The program is developing multiple laboratories in order to produce MDLs tailored for partner nation-unique requirements, some of which will have more high-fidelity signal generator channels earlier than the USRL. The program is considering using one of these other laboratories for Block 3F MDL development and testing; however, the MDL that will be used for IOT&E must be developed, verified, validated, and tested using operationally representative procedures, like the MDLs that will be developed for the operational aircraft in the USRL.

Weapons Integration and Demonstration Events

- Block 3F weapons delivery accuracy (WDA) events are not complete. These events, required by the TEMP, are key developmental test activities necessary to ensure the full fire-control capabilities support the "find, fix, track, target, engage, assess" kill chain. As of the end of November, only 5 of the 26 events (excluding the gun events) had been completed and fully analyzed. Several WDAs have revealed deficiencies and limitations to weapons employment (e.g., AIM-9X seeker status tone problems and out-of-date launch zones for AIM-120 missiles). An additional 11 WDAs had occurred, but analyses were ongoing. Of the 10 remaining WDAs that had not been completed, 4 were still blocked due to open deficiencies that must be corrected before the WDA can be attempted. However, the program did not have time to fix the deficiencies, complete the remaining WDAs and analyze them before finalizing Block 3FR6 in late November for flight testing to begin in December 2016. For example, recent F-35C flight testing to prepare for a weapons event with the C-1 version of the Joint Stand-Off Weapon (JSOW-C1) discovered weapon integration, Pilot Vehicle Interface (PVI) and mission planning problems that will prevent full Block 3F combat capability from being delivered, if not corrected. These discoveries were made too late to be included in the Block 3FR6 software, the final planned increment of capability delivered to flight test for SDD. Also, multiple changes are being made late in Block 3F development to mission systems fire control software to correct problems with the British AIM-132 Advanced Short-Range Air-to-Air Missile (ASRAAM) missile and Paveway IV bomb, changes which could affect the U.S. AIM-9X air-to-air missile and GBU-31 laser-guided bomb capabilities, and may require regression testing of the U.S. weapons.
- Block 3F adds gun capability for all variants. The F-35A gun is internal; the F-35B and F-35C each use a gun pod. Ground firing tests have been completed on all variants; only on the F-35A has initial flight testing of the gun been accomplished. Early testing of the air-to-ground and air-to-air symbology have led to discovery of deficiencies in the gunsight and strafing symbology displayed in the pilot's helmet – deficiencies which may need to be addressed before accuracy testing of the gun, aimed by the HMDS, can be completed. Because of the late testing of the gun and the likelihood of additional discoveries, the program's ability to deliver gun capability with Block 3F before IOT&E is at risk, especially for the F-35B and F-35C.

Pilot Escape System

- The program completed pilot escape system qualification testing in September 2016, which included a set of modifications designed to reduce risk to pilots weighing less than 136 pounds.
  - Modifications include:
    - Reduction in the weight of the pilot's Generation III Helmet Mounted Display System (HMDS), referred to as the Gen III Lite HMDS
    - Installation of a switch on the ejection seat which allows lighter-weight pilots to select a slight delay in the activation of the main parachute
    - Addition of a Head Support Panel (HSP) between the risers of the parachute.
  - These modifications to the pilot escape system were needed after testing in CY15 showed that the risk of serious injury or death is greater for lighter-weight pilots. Because of the risk, the Services decided to restrict pilots weighing less than 136 pounds from flying the F-35.

- Twenty-two qualification test cases were completed between October 2015 and September 2016, with variations in manikin weight, speed, altitude, helmet size and configuration, and seat switch setting. Data from tests showed that the HSP significantly reduced neck loads under conditions that forced the head backwards, inducing a rearward neck rotation, during the ejection sequence. Data also showed that the seat switch reduced the "opening shock" by slightly delaying the main parachute for lighter-weight pilots at speeds greater than 160 knots. The extent to which the risk has been reduced for lighter-weight pilots (i.e., less than 136 pounds) by the modifications to the escape system and helmet is still to be determined by a safety analysis of the test data. If the Services accept the risk associated with the modifications to the escape system for the lighter-weight pilots, restrictions will likely remain in effect until aircraft have the modified seat and the HSPs, and until the lighter-weight Gen III Lite helmets are procured and delivered to the applicable pilots.
- Based on schedules for planned seat modifications, production cut-in of the modified seat, and the planned delivery of the Gen III Lite HMDS, the Air Force may be able to reopen F-35 pilot training to lighter-weight pilots (i.e., below 136 pounds) in early 2018. DOT&E is not aware of the plans for the Marine Corps and the U.S. Navy to open F-35 pilot training to the lighter-weight pilots.
- Part of the weight reduction to the Gen III Lite HMDS involved removing one of the two installed visors (one dark, one clear). As a result, pilots that will need to use both visors during a mission (e.g., during transitions from daytime to nighttime) will have to store the second visor in the cockpit. However, there currently is not enough storage space in the cockpit for the spare visor, so the program is working a solution to address this problem.
- The program has yet to complete the additional testing and analysis needed to determine the risk of pilots being harmed by the Transparency Removal System (which shatters the canopy first, allowing the seat and pilot to leave the aircraft) during off-nominal ejections in other than ideal, stable conditions (such as after battle damage or during out-of-control situations). Although the program completed an off-nominal rocket sled test with the Transparency Removal System in CY12, several aspects of the escape system have changed since then (including significant changes to the helmet) which warrant additional testing and analyses.

Joint Simulation Environment (JSE)

- JSE is a man-in-the-loop, F-35 mission systems software-in-the-loop simulation being developed to meet the operational test requirements for Block 3F IOT&E. However, multiple aspects of the JSE development effort continue to fall significantly behind schedule. The Program Office has been negotiating with the contractor to receive the F-35 aircraft and sensor models, referred to as "F-35 In A Box (IAB)," but very limited progress was made in CY16. Also, delays with security clearances for new personnel limited progress on several aspects of the development and validation effort. Although the Naval Air Systems Command (NAVAIR) government team has begun installing hardware on their planned timeline (facilities, cockpits, etc.), the team's progress in integrating the many different models (i.e., multi-spectral environment, threats, weapons) with F-35 IAB has been severely limited, and the verification, validation and accreditation of these models within JSE for use in IOT&E, have effectively stalled. The F-35 program's JSE schedule indicates that it plans to provide a fully accredited simulation for IOT&E use in May 2019; a schedule that carries high risk of further slips without resolving these issues, and is not credible. Without a high-fidelity simulation, the F-35 IOT&E will not be able to test the F-35's full capabilities against the full range of required threats and scenarios. However, for the reasons above, it is now clear that the JSE will not be available and accredited in time to support the Block 3F IOT&E. Therefore, the recently approved IOT&E detailed test design assumes only open-air flight testing will be possible and attempts to mitigate the lack of an adequate simulation environment as much as possible. In the unlikely event the JSE is ready and accredited in time for IOT&E, the test design has JSE scenarios that would be conducted.

Live Fire Test and Evaluation (LFT&E)

- The F-35 LFT&E program completed one major live fire test series using an F-35C variant full-scale structural test article (CG:0001). Preliminary test data analyses:
  - Demonstrated the tolerance of the vertical tail attachments to high-explosive incendiary (HEI) projectile threats
  - Confirmed the tolerance of the aft boom structures to Man-Portable Air Defense System (MANPADS) threats
  - Demonstrated vulnerabilities to MANPADS-generated fires in engine systems and aft fuel tanks. The data will support a detailed assessment in 2017 of these contributions to overall F-35 vulnerability.
- The test plan to assess chemical and biological decontamination of pilot protective equipment is not adequate; no plans have been made to test either the Gen II or the Gen III HMDS. The Program Office is on track to evaluate the chemical and biological agent protection and decontamination systems in the full-up system-level decontamination testing in FY17.
- The Navy conducted vulnerability testing of the F-35B electrical and mission systems to electromagnetic pulses (EMP).
- The 780th Test Squadron at Eglin AFB, Florida completed ground-based lethality tests of the PGU-47/U Armor Piercing High Explosive Incendiary with Tracer (APHEI-T) round, also known as the Armor Piercing with Explosive (APEX), against armored and technical vehicles, aircraft, and personnel-in-the-open targets.

Suitability

- The operational suitability of all variants continues to be less than desired by the Services. Operational and training

units must rely on contractor support and workarounds that would be challenging to employ during combat operations. In the past year some metrics of suitability performance have shown improvement, while others have been flat or declined.
- Most metrics still remain below interim goals to achieve acceptable suitability by the time the fleet accrues 200,000 flight hours, the benchmark set by the program and defined in the Operational Requirements Document (ORD) for the aircraft to meet reliability and maintainability requirements.
- Reliability growth has stagnated and, as a result, it is highly unlikely that the program will achieve the ORD threshold requirements at maturity for the majority of reliability metrics, most notably Mean Flight Hours Between Critical Failures, without redesigning components of the aircraft.

Autonomic Logistics Information System

- The program failed to release any new ALIS capability in 2016, but did release two updates to the currently fielded ALIS 2.0.1 software to address deficiencies and usability shortfalls. The program planned to test and field ALIS 2.0.2, including integration of propulsion data management, in the summer of 2016, to support the Air Force declaration of Initial Operational Capability; however, delays in development and integration have pushed the testing and fielding into 2017.
- Because of the delays with ALIS 2.0.2, Lockheed Martin shifted personnel to support that product line development. This caused delays in the development schedule of ALIS 3.0, the last major SDD software release. The program acknowledged in August 2016 that it could not execute the ALIS 3.0 schedule and developed plans to restructure this ALIS release and the remaining planned ALIS capabilities into multiple releases, including some that will occur after SDD completion.
  - The program's restructuring of the ALIS capability delivery plan divided the planned capabilities and security updates for ALIS into four more versions: one version for SDD (ALIS 3.0), with what the Program Office considered to be needed for IOT&E, and three additional software releases intended to be fielded at 6-month intervals after SDD completion, with the remaining content originally planned for ALIS 3.0.
  - The program plans to release software maintenance updates midway between each of these four software releases to address deficiencies and usability problems, but these releases will not include new capabilities.
- The Air Force completed its first deployment of F-35A aircraft using the modularized version of the ALIS squadron hardware, called the Standard Operating Unit Version 2 (SOU v2), and software release 2.0.1 to Mountain Home AFB, Idaho in February 2016. Difficulties integrating the SOU v2 into the base network interfered with connectivity between the SOU v2 and the Mountain Home-provided workstations, but did not affect connectivity of the SOU v2 with the main Autonomic Logistics Operating Unit (ALOU) in Fort Worth, Texas.

Air-Ship Integration and Ship Suitability

- The program completed the last two ship integration DT periods in 2016 – both referred to as "DT-III" – one with the F-35B in November aboard the amphibious assault ship USS *America,* and one with the F-35C in August aboard the aircraft carrier USS *George Washington*. Test objectives included expanding the flight clearances for shipboard operations with carriage of external weapons, night operations, and Joint Precision Approach Landing System (JPALS) integration testing. For both periods, operational and test units accompanied the deployment to develop concepts of operations for at-sea periods.
- The specialized secure space set aside for F-35-specific mission planning and the required Offboard Mission Support (OMS) workstations is likely unsuitable for regular Air Combat Element (ACE) operations on the Landing Helicopter Dock (LHD) and Landing Helicopter Assault (LHA)-class assault ships with the standard complement of six F-35B aircraft, let alone F-35B Heavy ACE configurations with more aircraft. Similarly, for F-35C operations onboard CVN, adequate secure spaces will be needed to ensure planning and debriefing timelines support carrier operations.
- The F-35C DT-III included external stores, including bombs, but only pylons with no AIM-9X missiles on the outboard stations (stations 1 and 11) due to the F-35C wingtip structural deficiency. The U.S. Navy directed a proof-of-concept demonstration of an F-35C engine change while underway, a process that took several days to complete. ALIS was not installed on USS *George Washington*, so reach-back via satellite link to the shore-based ALIS unit was required, similar to previous F-35C test periods at sea, but connectivity proved troublesome.
- The F-35B DT-III deployment included an engine installation due to required maintenance, along with a lift fan change proof-of-concept demonstration. The Marine Corps deployed with an operational SOU v2 on USS *America*.

Cybersecurity Testing

- The JSF Operational Test Team (JOTT) continued to conduct cybersecurity testing on F-35 systems, in partnership with certified cybersecurity test organizations and personnel, and in accordance with the cybersecurity strategy approved by DOT&E in February 2015. In 2016, the JOTT conducted adversarial assessments (AA) of the ALIS 2.0.1 SOU, also known as the Squadron Kit, at Marine Corps Air Station (MCAS) Yuma, Arizona, and the Central Point of Entry (CPE) at Eglin AFB, Florida, completing testing that began in the Fall of 2015. They also completed cooperative vulnerability and penetration assessments (CVPA) of the mission systems ALOU at Edwards AFB, California, used to support developmental testing, and the operational ALOU in Fort Worth, Texas. The JOTT, with support from the

Air Force Research Laboratory (AFRL) also completed a limited cybersecurity assessment of the F-35 air vehicle in September 2016, on an F-35A aircraft assigned to the operational test squadron at Edwards AFB. These tests were not conducted concurrently as originally planned, so end-to-end testing of ALIS, from the ALOU to the air vehicle, has not yet been accomplished. An AA of the operational ALOU was scheduled for early December 2016, which would complete a full assessment (CVPA and AA) of each ALIS 2.0.1 component.

- The cybersecurity testing in 2016 showed that the program has addressed some of the vulnerabilities identified during earlier testing periods; however, much more testing is needed to assess the cybersecurity structure of the air vehicle and supporting logistics infrastructure system (i.e., ALOU, CPE, Squadron Kit) and to determine whether, and to what extent, vulnerabilities may have led to compromises of F-35 data. The scope of the cybersecurity testing must also expand to include other systems required to support the fielded aircraft, including the Multifunction Analyzer Transmitter Receiver Interface Exerciser (MATRIX) system which is used by contractor maintenance technicians, the USRL, avionics integration labs, the OMS and training simulators.

Follow-on Modernization

- The program continued making plans for Follow-on Modernization (FoM) for all variants, also referred to as Block 4, which is on DOT&E oversight. The program intends to award the contract for the modernization effort in 2QCY18 with developmental flight testing beginning in 3QCY19. Four increments of capability are planned, Blocks 4.1 through 4.4. Blocks 4.1 and 4.3 will provide software-only updates; Blocks 4.2 and 4.4 will include significant avionics hardware changes as well as software updates. Improved Technical Refresh 3 (TR3) processors with open architecture, designed to make adding, upgrading and replacing components easier, are planned to be added in Block 4.2.
- The program's plans for FoM are not executable for a number of reasons including, but not limited to the following:
  - Too much technical content for the production-schedule-driven developmental timeline
  - Overlapping increments without enough time for corrections to deficiencies from OT to be included in the next increment
  - High risk due to excessive technical debt and deficiencies from the balance of SDD and IOT&E being carried forward into FoM because the program does not have a plan or funding to resolve key deficiencies from SDD prior to attempting to add the planned Block 4.1 capabilities
  - Inadequate test infrastructure (aircraft, laboratories, personnel) to meet the testing demands of the capabilities planned and the multiple configurations (i.e., TR2, TR3, and Foreign Military Sales)
  - Insufficient resources for conducting realistic operational testing of each increment

System

- The F-35 Joint Strike Fighter (JSF) program is a tri-Service, multi-national, single-seat, single-engine family of strike aircraft consisting of three variants:
  - F-35A Conventional Take-Off and Landing (CTOL)
  - F-35B Short Take-Off/Vertical-Landing (STOVL)
  - F-35C Aircraft Carrier Variant (CV).
- The F-35 is designed to survive in an advanced threat environment (year 2015 and beyond) using numerous advanced capabilities. It is also designed to have improved lethality in this environment compared to legacy multi-role aircraft.
- Using an active electronically scanned array (AESA) radar and other sensors, the F-35 with Block 3F is intended to employ precision-guided weapons, such as the GBU-12 Laser-Guided Bomb (LGB), GBU-31/32 Joint Direct Attack Munition (JDAM), GBU-39 Small Diameter Bomb (SDB), Navy Joint Stand-Off Weapon (JSOW)-C1, and air-to-air missiles such as AIM-120C Advanced Medium-Range Air-to-Air Missile (AMRAAM), and AIM-9X infrared guided short-range air-to-air missile.
- The SDD program was designed to provide mission capability in three increments:
  - Block 1 (initial training; two increments were fielded: Blocks 1A and 1B)
  - Block 2 (advanced training in Block 2A and limited combat capability in Block 2B)
  - Block 3 (limited combat capability in Block 3i and full SDD warfighting capability in Block 3F)
- The F-35 is under development by a partnership of countries: the United States, Great Britain, Italy, the Netherlands, Turkey, Canada, Australia, Denmark, and Norway.

Mission

- The Combatant Commander will employ units equipped with F-35 aircraft in joint operations to attack targets during day or night, in all weather conditions, and in heavily defended areas.
- The F-35 will be used to attack fixed and mobile land targets, surface units at sea, and air threats, including advanced aircraft and cruise missiles.

Major Contractor

Lockheed Martin, Aeronautics Division – Fort Worth, Texas

Test Strategy, Planning, and Resourcing

- Preparations for IOT&E. In 2016, the JPO acknowledged schedule pressure for starting IOT&E in August 2017, as planned in the Integrated Master Schedule created in 2012. Due to multiple problems and further delays, the program will not be able to start IOT&E until late CY18, at the earliest, and more likely early CY19, but it could be as late as CY20 before required modifications are completed to IOT&E aircraft. The issues that will not allow IOT&E to start as planned include:
  - Continued schedule delays in completing Block 3F mission systems development and flight testing
    - The program's plan to deliver the "Full SDD Warfighting Capability" version of Block 3F software – now referred to as version 3FR6 – was significantly delayed. It was planned for release to flight test in February 2016, according to the program's latest mission systems software and capability release schedule, but did not begin flight test until early December 2016 (10 months late). However, during this time, the program released several "Quick Reaction Cycle" (QRC) versions of software to quickly resolve deficiencies that were preventing the completion of key test points, like weapons deliveries. Due to these delays, along with the recently acknowledged SDD funding shortfall, software versions 3FR7 and 3FR8 have fallen off the program's schedule. However, ongoing delays in maturing some of the capabilities and new problem discoveries continue to prevent testing of some planned Block 3F capabilities and will almost certainly require additional unplanned releases of Block 3F software.
    - DOT&E estimates that mission systems flight testing will not complete prior to July 2018, based on the number of Block 3F baseline mission systems test points to go, the monthly average mission systems test point completion rate observed for CY16 to date, and the average regression, discovery and developmental test point rate of 63 percent experienced so far in CY16. This estimate also includes a decrement of 11 percent for test points to be designated "no longer required," the percentage used by the Program Office to account for efficiency in CY16 planning of test point accomplishment objectives.
  - Delayed and incomplete Block 3F developmental testing Weapons Delivery Accuracy (WDA) events and ongoing weapons integration issues
    - WDA events – key developmental test activities necessary to ensure the full fire-control capabilities work together to properly support the "find, fix, track, target, engage, assess" kill chain – are not complete. As of the end of November, only 5 of the 26 WDA events (excluding gun events) had been completed and fully analyzed.
    - Several WDAs have revealed deficiencies and limitations to weapons employment (e.g., AIM-9X seeker status tone problems and out-of-date launch zones for AIM-120 missiles). An additional 11 WDAs had occurred, but analyses are ongoing. Of the 10 remaining WDAs, 4 were still blocked due to open deficiencies that must be corrected before the WDA can be attempted, but the program did not have time to complete and analyze them before finalizing Block 3FR6.
  - Continued delays in completing flight sciences test points, particularly those needed to provide the F-35B Block 3F flight envelope for operational use
    - Through the end of November, flight sciences testing on all variants was behind the plan for the year. Although the program planned to complete Block 3F testing on the F-35A in October, testing continued into December, with weapons separations and regression testing of new software to be completed.
    - Flight sciences test point completion for CY16 was 5 percent behind for the F-35B and 23 percent behind for the F-35C as of the end of November. The program plans to complete Block 3F flight sciences testing in August 2017 with the F-35C and by the end of October 2017 with the F-35B, the latter being 10 months later than planned in the program's Integrated Master Schedule.
    - Due to the delays with completing flight sciences testing, the program plans a phased release of the Block 3F envelope across all three variants, with the full Block 3F envelope for the F-35B not being released until mid-CY18.
  - Further delays in completing gun testing for all three variants and recently discovered gunsight deficiencies
    - Block 3F adds gun capability for all three variants. The F-35A gun is internal; the F-35B and F-35C each use a gun pod. Differences in mounting make the gun pods unique to a specific variant, i.e., a gun pod designated for an F-35B cannot be mounted on an F-35C aircraft. Flight sciences testing of the gun has occurred with the F-35A; discoveries required control law changes to the flight control software and delayed the start of mission systems gun testing on the F-35A from September 2016 to December 2016. Although the F-35B and F-35C have completed ground firings of their gun pods, airborne flight sciences gun testing (i.e., airborne firing) for the F-35B and F-35C has yet to be accomplished.
    - Besides the ongoing delays with software and gun modifications, both DT and OT pilots have reported concerns from preliminary test flights that the air-to-ground gun strafing symbology, displayed in the helmet, is currently operationally unusable and potentially unsafe to complete the planned testing due to a combination of symbol clutter obscuring the target, difficulty reading key information, and pipper stability. Also, for air-to-air employment, the pipper symbology is very unstable while tracking a target aircraft; however, the funnel version of the air-to-air gunsight appears to be more stable in early testing.
    - Fixing these deficiencies may require changes to the mission systems software that controls symbology

to the helmet, or the radar software, even though the program recently released the final planned version of flight test software, Block 3FR6. Plans to begin flight testing of aimed gunshots, integrated with mission systems, which requires aiming with the helmet, on the F-35A were planned for fall of 2016, but had slipped to December 2016, at the soonest, before this new problem with the gun symbology was discovered.
    - F-35B ground test firing of its gun pod was accomplished in July 2016 and flight testing is planned to begin in January 2017; the F-35C conducted first ground firing in November 2016; flight testing is planned to begin in March 2017.
- Late availability of verified, validated and tested Block 3F MDLs
    - Failure by the program to plan for, procure, and provide the necessary Block 3F upgrades and the associated Mission Data File Generation (MDFG) tools to the USRL has caused delays in developing, testing, and verifying mission data loads for IOT&E.
    - If Block 3F MDFG tools are delivered in early CY17, verified, validated and tested MDLs will not be available for IOT&E until June 2018 (15 months later) at the soonest, which is late to need for both IOT&E and fielding of Block 3F.
    - In collaboration with partner nations, the program is developing multiple laboratories to produce MDLs tailored for country-unique requirements. Although these other laboratories may provide additional capacity for developing and testing MDLs, the MDL that will be used for IOT&E must be developed, verified, validated, and tested using operationally representative procedures involving the USRL.
- Continued shortfalls and delays with ALIS and late delivery of ALIS software version 3.0, the final planned version for SDD, which is at risk of slipping from early-CY18 into mid-CY18
    - The program has failed to deliver increments of ALIS capability as planned. No new capability has completed testing in 2016, although the program had planned to field ALIS 2.0.2, with the propulsion integration module included, by August 2016 to support the Air Force IOC declaration, but continued problems caused this to slip into early CY17.
    - The program restructured the ALIS capabilities delivery plan in 2016 and moved content planned for ALIS 3.0 – the last version to be developed during SDD – to post-SDD ALIS development and fielding. Despite the delays and deferred content, IOT&E will still evaluate the suitability of the F-35 with ALIS in operationally realistic conditions.
- Significant, well-documented deficiencies resulting in overall ineffective operational performance of Block 3F, hundreds of which will not be adequately addressed with fixes and corrections verified with flight testing within SDD
    - The program, Services, JOTT, and DT and OT pilots recently conducted a review of the status and priority of open deficiency reports (DRs). This review was a follow-on from a review in the spring of 2016, where the stakeholders reviewed all the open DRs and created a rank-ordered list of 263 priority deficiencies to be addressed by the program. The review team later pared the list down to 176 priority DRs, with 12 being brought forward to the JPO's Configuration Steering Board (CSB); 7 for decision and 5 for CSB awareness. In the review in the fall of 2016, the stakeholders reviewed the approximately 1,200 open deficiencies, including the original 176 priority DRs, plus 231 new DRs since Feb 2016, minus 55 that had been corrected, to create an updated DR list. This time, however, the team prioritized the open DRs into one of 4 priorities: priority 1 DRs are "service critical," and the Services will not field the aircraft unless these DRs are fixed; priority 2 have significant impact that may, when combined with other DRs, lead to mission failure; priority 3 carry medium impact and should be addressed by the program, but maybe not within SDD; and priority 4 have low impact. The review team identified 72 DRs as priority 1 and 204 DRs as priority 2, for a total of 276 DRs to address within SDD or risk fielding deficiencies that could lead to operational mission failures during IOT&E or combat.
    - While these deficiencies must be addressed to some degree during the remaining time in development, the final planned software load, Block 3FR6, which started flight test in December 2016, only included attempted fixes for less than half of the 276 priority 1 and 2 DRs. Corrections to these deficiencies will need to be developed, tested in the labs (if possible) and then flight tested, since the labs have proven to not be an adequate test venue for verifying corrections to deficiencies identified during flight testing. However, the current schedule-driven program plans to close out SDD testing in 2017 do not include enough time to fix these key deficiencies, nor time to verify corrections in flight test. There is risk in attempting to verify DR fixes only in the lab because the labs proved to not always be representative of the actual aircraft for detecting problems or verifying fixes for stability problems. The labs are also not able to adequately replicate the demands on the mission systems like open air testing does, such as infrared and radar background clutter and terrain-driven multipath reflections of radio-frequency emissions from threat emitters, so most fixes to deficiencies will require flight testing.
- Overall ineffective operational performance with multiple key Block 3F capabilities to date
    - Three independent assessments conducted during the past 6 months rate the F-35 as red or unacceptable (not all assessments used the same scoring criteria) in most critical combat mission areas: The Air Force's IOC Readiness Assessment (IRA) of Block 3i, an OT

community assessment of Block 3FR5.03 based on observing develomental testing, and an assessment by the JOTT of the capability of Block 3FR5.05 to perform the planned mission trials in the IOT&E, based on observing and assisting with DT.
- In July, the Air Force completed their IRA report. The assessment was based on a limited series of events conducted with six Block 3i-configured aircraft, including test missions in Close Air Support (CAS), Air Interdiction (AI), and Suppression/Destruction of Enemy Air Defenses (SEAD/DEAD). The assessment noted unacceptable problems in fusion and electronic warfare and, concerning the CAS mission, determined that the Block 3i F-35A does not yet demonstrate equivalent CAS capabilities to those of fourth generation aircraft.
- In August, an F-35 OT pilot from Edwards AFB, California, briefed the results of an OT community assessment of F-35 mission capability with Block 3FR5.03, based on observing developmental flight test missions and results to date. This OT assessment rated all IOT&E mission areas as "red," including CAS, SEAD/DEAD, Offensive Counter Air (OCA) and Defensive Counter Air (DCA), AI, and Surface Warfare (SuW). Several DT Integrated Product Team representatives also briefed the status of different F-35 mission systems capabilities, most of which were rated "red," and not meeting the entrance criteria to enter the "graduation level" mission effectiveness testing. Trend items from both the OT and IPT briefings were limitations and problems with multiple Block 3F system modes and capabilities, including Electro-Optical Targeting System (EOTS), Distributed Aperture System (DAS), radar, electronic warfare, avionics fusion, identification capabilities, navigation accuracy, GPS, datalinks, weapons integration and mission planning.
- In November 2016, the JOTT provided an assessment of a later version of Block 3F software – version 3FR5.05 – based on observing and assisting with F-35 DT flight operations and maintenance. The JOTT assessment made top-level, initial predictions of expected IOT&E results of the F-35 with Block 3FR5.05 against planned scenarios and realistic threats. For mission effectiveness, the assessment predicted severe or substantial operational impacts across all the planned IOT&E missions (similar to the list of missions above) due to observed shortfalls in capabilities, with the exception of the Reconnaissance mission area, which predicted minimal operational impact. Unlike the other assessments, the JOTT also assessed suitability, predicting mixed operational impacts due to shortfalls for deployability (from minimal to severe), severe impacts for mission generation, and substantial impacts for training and logistics support.

- Continued low aircraft availability, especially for the early production lot IOT&E aircraft. The program has still not been able to improve aircraft availability, in spite of reliability and maintainability initiatives, to the goal of 60 percent, which is well short of the 80 percent necessary to conduct an efficient IOT&E and to support sustained combat operations. As a result, IOT&E will likely take longer than currently planned and suitability, along with fielded operations, will be adversely affected.
- Late delivery of the JSE, a man-in-the-loop simulator expected for IOT&E, which required the test team to create a test design that attempts to mitigate the high likelihood that it will not be available. Some IOT&E measures of effectiveness will not be fully resolved without a verified, validated and accredited simulator to evaluate the F-35 in an operationally realistic, dense threat environment.
- Progress in verification of Joint Technical Data (JTD) is behind plans to complete within SDD, particularly those for troubleshooting aircraft fault codes and for support equipment. As of September 2016, the program had verified approximately 83 percent of all JTD modules, but just over 50 percent of those associated with support equipment. While symptomatic of an immature system, the lack of verified JTD makes the completion of aircraft maintenance more difficult and forces maintainers to rely more heavily on submitting electronic requests to the contractor for help or to seek assistance from contractor representatives at field locations.
  - The program has made significant progress in verifying JTD for sustaining the aircraft's low observable signature, primarily by completing verifications on an F-35A damaged in 2014 by an engine fire
  - All Block 3F JTD must be written and verified prior to the start of IOT&E
- Delays in completing the extensive and time-consuming modifications required to the fleet of operational test aircraft which, if not mitigated with an executable plan and contract, could significantly delay the start of IOT&E.
  - The program is developing and working plans with Lockheed Martin and the Services to provide production-representative operational test aircraft, with the necessary instrumentation, to start IOT&E. Although it was part of the agreed-to entrance criteria for IOT&E, the program currently does not have an adequate plan to provide test aircraft that meet the TEMP criteria for entering IOT&E until late-2018, at the earliest, and possibly as late as 2020. Extensive modifications are required on all of the TEMP-designated OT aircraft; 155 different modifications (known to date) are necessary between all variants and all lots of aircraft (Lots 3 through 5) to bring the IOT&E aircraft to the required production-representative configuration, although no single aircraft requires all 155 modifications. Additional discoveries and modifications are likely as the program finishes SDD.
  - The Program Office and the Services are considering using later lot aircraft with an alternate instrumentation package. However, to date, no analyses of the adequacy of the alternate instrumentation has been completed; nor is there a contract to design, build and test alternative packages.
- Insufficient progress in the development and testing of modeling, simulations, and instrumentation required for IOT&E.

  - Flight testing to allow the Data Acquisition Recording and Telemetry (DART) pod to be used throughout the full Block 3F flight envelope during IOT&E, including during simulated weapons releases when the weapons bay doors will cycle open, has not yet been planned, put on contract or completed. The DART pod is required for collecting data during IOT&E.
  - Flight testing of the Air-to-Air Range Infrastructure (AARI) – as integrated with the F-35 and required for adequacy of the open air flight test trials – has not yet been completed. AARI is used to support battle-shaping of air-to-air engagements by modeling weapon fly-outs and accounting for endgame effects to remove aircraft "shot down" by another aircraft or ground threat. The program must begin testing AARI and allow for corrections of deficiencies during flight testing, to ensure AARI is adequate for IOT&E.
  - Integration of AARI and associated range simulators with the F-35 to indicate inbound missiles on cockpit displays is required for an adequate evaluation of open air missions. Within the aircraft, the Embedded Training (ET) function is intended to support live/virtual/constructive training using a mixture of real and virtual entities (e.g., missiles, ground systems, and aircraft). To avoid intermingling data from real and virtual entities, as it may cause issues within the F-35, the contractor developed a separate model, the Fusion Simulation Model (FSM), to emulate fusion functionality for virtual entities within ET. The current FSM implementation has significant deficiencies that make the model so inaccurate that some required capabilities may not be usable for IOT&E. Although a properly functioning FSM is required for IOT&E, the program had not yet completed contract actions for fixes to correct the FSM deficiencies within SDD and prior to IOT&E, but was apparently developing plans and intended to award contract actions for at least some of the work on FSM by the end of January 2017.
  - Virtual Threat Insertion (VTI) is a function inside of FSM that correlates virtual threat parametric data supplied by AARI with data from tables embedded within the FSM to provide cockpit display indications to the pilot for threat activity (i.e., a surface-to-air missile launched). The reference tables for VTI are incomplete and do not include all threats planned for use in IOT&E. The program was also apparently planning to update the VTI tables, but this was also not yet on contract.
  - The Logistics Composite Model (LCOM), which will be used to support assessments of suitability measures including sortie generation rate and logistics footprint – two key performance parameters in the ORD – is still under development. Seven versions of the model will be needed to cover the three variants as well as partner-unique and shipborne operations.
- The program is behind in developing and fielding training simulators, referred to as F-35 Full Mission Simulators (FMS), to train pilots, both at the integrated training centers for initial F-35 pilot training and at the operational locations. The FMS is a multi-ship, man-in-the-loop, F-35 mission systems software-in-the-loop simulation using virtual threats, it is used to train both U.S. and partner pilots.
  - In 2014, the program moved simulator development from Akron, Ohio to Orlando, Florida. As a result of the move, the program lost experienced personnel, suffered from shortfalls in required staffing, and fell behind in meeting the hardware and software demands of the rapidly growing pilot training requirements.
  - In March 2016, following an inspection of the Block 2B FMS, evaluators reported 203 test discrepancies; 173 remained open, 4 were canceled, 2 were pending corrections, and 24 had been closed and corrections included in the next build of FMS for Block 3i.
  - The Block 3i FMS is behind the planned schedule for fielding. The first Block 3i FMS is scheduled for delivery to Marine Corps Air Station Iwakuni, Japan, in December 2016, followed by two more FMS delivered to partner countries.
  - Because of delays in delivering the Block 3i FMS, the Block 3F FMS is even further behind schedule. Although earlier plans included delivering the Block 3F FMS in CY17, the program is now replanning the schedule.
  - Since the FMS runs F-35 mission systems software, it requires Block 3F mission data files, integrated with virtual threats, to build the threat environment simulation (TES). It currently takes up to 20 months for the program to build the TES after new mission data files are available, hence pilots will not have Block 3F FMS, with the USRL-produced mission data files, available for training prior to IOT&E. Alternatively, the program may elect to use the contractor-developed DT mission data files for the Block 3F FMS. However, doing so would make the training in the FMS not operationally representative, as those mission data files do not accurately portray the TES to the pilot. Without an adequate Block 3F FMS, the OT pilots will have to rely on the available Block 3F OT aircraft for training.

- The JOTT completed detailed test designs for accomplishing IOT&E. DOT&E approved the designs in August 2016. The test designs include comparisons of the F-35 with the A-10 in the Close Air Support role, the F-16C (Block 50) in the Suppression/Destruction of Enemy Air Defenses (SEAD/DEAD) mission area, and the F-18E/F in the air-to-surface strike mission area. The JOTT has begun detailed test planning based on these designs, and will provide these plans to DOT&E for approval, prior to the start of IOT&E.
- Block Buy. The program and Services continue to pursue a "Block Buy" for production lots 12 through 14. This multi-year procurement scheme is based on a partial group of the partner nations, designated as "Full Participants," funding a 2 percent Economic Order Quantity (EOQ) in FY17 and another 2 percent EOQ in FY18. Other partner nations,

designated "Partial Participants," would procure Lot 12 as a single year lot procurement, then commit to procuring Lots 13 and 14 as a part of the Block Buy and provide funding of 4 percent EOQ in FY18. Similar to the Partial Participants, the Services would procure Lot 12 as a single year procurement and fund 4 percent EOQ in FY18, but maintain the options for single year procurements in Lots 13 and 14. Altogether, 452 F-35 aircraft would be procured under the Block Buy scheme, on top of the 490 aircraft (346 for the U.S. Services) previously procured in lots 1-11, all purchased without the informed results of an IOT&E. As reported in the FY15 DOT&E Annual Report, many questions remain on the prudence of committing to the multi-year procurement of a Block Buy scheme prior to the completion of IOT&E:

- Is the F-35 program sufficiently mature to commit to the Block Buy with the ongoing rate of discovery while in development?
- Is it appropriate to commit to a Block Buy given that essentially all the aircraft procured thus far require modifications to be used in combat? The Services will have accepted delivery of 346 aircraft through Lot 11, before the additional aircraft are purchased via the Block Buy scheme.
- Would committing to a Block Buy prior to the completion of IOT&E provide the contractor with needed incentives to fix the problems already discovered, as well as those certain to be discovered during IOT&E?
- Would the Block Buy be consistent with the "fly before you buy" approach to acquisition advocated by the Administration, as well as with the rationale for the operational testing requirements specified in title 10, U.S. Code, or would it be considered a "full rate" decision before IOT&E is completed and reported to Congress, not consistent with the law?

• Follow-on Modernization (FoM). The program continued making plans for all variants for FoM, also referred to as Block 4, which is on DOT&E oversight. The program intends to award the contract for the modernization effort in 2QCY18 with developmental flight testing beginning 3QCY19. Four increments of capability are planned, Blocks 4.1 through 4.4. Blocks 4.1 and 4.3 will provide software-only updates, Blocks 4.2 and 4.4 will add hardware as well as software updates. Improved Technical Refresh 3 (TR3) processors are planned to be added in Block 4.2. However, the plans for FoM are not executable for a number of reasons including, but not limited to, the following:
  - Too much technical content for the allocated developmental timeline. Experience with the F-22 modernization program indicates the planned 18- to 24-month cycle for FoM is insufficient for the large number of planned additional capabilities; the F-22 increments had less content plus software maintenance releases between new capability releases.
  - High risk of carrying excessive technical debt and deficiencies from Block 3F and the balance of SDD into FoM. The planned 4-year gap between the planned final release of Blocks 3F in 2017 and Block 4.1 in 2021 lacks resources (i.e., funding and time) for a bridge software maintenance release to reduce technical debt and verify Block 3F IOT&E corrections of deficiencies. Although the unresolved technical debt is an SDD shortfall, it sets up FoM to fail due to unrealistic planning and inadequate resourcing.
  - Insufficient time for conducting adequate operational testing for each increment.
    ▪ The current plan for F-35 Block 4.2 only has 18 months for DT flight test and 6 months for OT&E, despite containing substantially more new capabilities and weapons than F-22 Block 3.2B.
    ▪ For comparison, the F-22 Block 3.2B program planned approximately two years for DT flight test and one year of OT&E spin-up and flight test; F-22 Blocks 3.1, 3.2A and 3.2B have suffered delays and problems accomplishing testing due to inadequate test resources and schedule.
  - Inadequate test infrastructure (aircraft, laboratories, personnel) to meet the testing demands of the capabilities planned.
    ▪ The current end-of-SDD developmental test aircraft drawdown plan is still being developed. However, any plan that significantly reduces the F-35 test force in 2017 and 2018 – precisely when the program needs this test force to finish the delayed SDD Block 3F Joint Test Plan (JTP) and correct remaining deficiencies with additional Block 3F updates in preparation for IOT&E – would result in shortfalls of the necessary resources to provide full Block 3F capability.
    ▪ A robust test force will also be required to be available through 2020 to correct the inevitable new discoveries from IOT&E and produce a final Block 3F software release that provides a stable foundation for adding the new Block 4.1 capabilities.
    ▪ The program plans to award contracts to start simultaneous development of Blocks 4.1 and 4.2 in 2018, well prior to completion of IOT&E and having a full understanding of the deficiencies that will emerge from IOT&E; without any budget or time to fix deficiencies from earlier development.
    ▪ The requirement to integrate and test multiple configurations simultaneously (TR2 and TR3) will require additional time, test aircraft, and lab resources; a problem that must be addressed as the program considers plans for the fleet of test aircraft for FoM.
    ▪ As of the writing of this report, the program's published FoM plan would have reduced test infrastructure from 18 DT aircraft and 1,768 personnel, which are still heavily tasked to complete ongoing Block 3F development, to just 9 aircraft and approximately 600 personnel to support FoM. Clearly, this plan is grossly inadequate. However, the program and Services were in the process of replanning the test infrastructure for FoM and had not yet provided the results.

  - Both the Air Force and the Navy conducted independent studies in 2016 to determine what infrastructure and test periods for FoM would be adequate. Neither report had been released as of the time of this report. DOT&E has requested to see the preliminary results of the Air Force study, but the Air Force has refused to provide them, citing the fact that the results are not final and the report is in draft.
- Significant technical and schedule risk due to Block 4.1 adding new capabilities to the already-stretched TR2 avionics hardware, along with Block 4.2 attempting to simultaneously migrate to a new open-architecture TR3 processor while adding many significant new capabilities.
  - For Block 4.1, the program plans to add multiple new capabilities to the TR2 avionics hardware, even though this architecture already has memory and processing limitations running the full Block 3F capabilities, resulting in avionics stability issues and capability limitations.
  - For Block 4.2, the program plans to simultaneously add multiple significant new software capabilities while migrating to a new avionics hardware configuration, including a new open-architecture TR3 processor and new electronic warfare (EW) hardware. This will be far more challenging than the program's problematic re-hosting of Block 2B software, designed to run on TR1 processors, on to TR2 processors to create Block 3i. Although no new capabilities were added in Block 3i, significant avionics stability issues were manifested due to technical debt and differences with the new architecture.
  - The program claims the new F-35 Block 4.2 software, which will be designed to run on new TR3 processors, will also be backward-compatible to run in the hundreds of early production aircraft with TR2 processors, but has not yet presented a plan to demonstrate this. Based on the current TR2 architecture capacity limitations with Block 3F, this claim is unlikely to be realized.
  - Instead of adding lab capacity to support testing of processor loads with the additional mission systems capabilities, the program plans to reduce the lab infrastructure supporting development. The program has already retired the Cooperative Avionics Test Bed aircraft – a decision that has increased the burden on flight testing with F-35 aircraft.
  - Current JPO projections for modifying aircraft with TR2 processors to the TR3 processor configuration extend into the 2030s. As a result, up to three configurations of test aircraft and labs may be needed if the program requires more advanced processors than the TR3 planned for Block 4 (i.e., the next Block upgrade requiring even more processing capacity driving the need for new processors).
  - The program also does not yet have an executable plan to provide a mission data reprogramming lab in the TR3 configuration in time to support Block 4.2 OT and fielding.
- Attempting to proceed with the current unrealistic plans for FoM would be to completely ignore the costly lessons learned from Block 2B, 3i and 3F development, as well as those from the F-22 program. As learned from the F-22 Blocks 3.1, 3.2A and 3.2B, an overly aggressive plan with inadequate resources ultimately takes longer, costs more and delays needed capabilities for the warfighter.

- This report includes assessments of the progress of testing to date, including developmental and operational testing intended to verify performance prior to the start of IOT&E. Test flights and test points are summarized in two tables on the next page.
  - For developmental flight testing, the program creates test plans by identifying specific test points (discrete measurements of performance under specific flight test conditions) for accomplishment, in order to assess the compliance of delivered capabilities with contract specifications.
    - Baseline test points refer to points in the test plans that must be accomplished in order to evaluate if performance meets contract specifications.
    - Non-baseline test points are accomplished for various reasons. Program plans include a budget for some of these points within the capacity of flight test execution. The following describes non-baseline test points.
      - » Development points are test points required to "build up" to, or prepare for, the conditions needed for assessing specification compliance (included in non-baseline budgeted planning in CY16).
      - » Regression points are test points flown to ensure that new software does not introduce shortfalls in performance for requirements that had previously been verified using previous software (included in non-baseline budgeted planning in CY16).
      - » Discovery points are test points flown to investigate root causes of newly discovered deficiencies or to characterize deficiencies so that the program can design fixes for them (not included in planning in CY16).
    - As the program developed plans for allocating test resources against test points in CY16, the program included a larger budget for non-baseline test points (development and regression points) for mission systems testing, as the plans for the year included multiple versions of software, requiring regression and developmental test points be completed. For CY16 mission systems testing, planners budgeted an additional 69 percent of the number of planned baseline test points for non-baseline test purposes (e.g., development and regression points), the largest margin planned for a CY to date. This large margin was planned because the program anticipated the test centers would need points for building up to the baseline points that would be flown for specification compliance as well as for completing regression of multiple versions of Block 3F software. In this report, growth in test points refers to points flown over and above the planned amount of baseline and budgeted non-baseline points (e.g., discovery points and any other added testing not originally included in the formal test plan).

- The continued need to budget for non-baseline test points in the CY16 plan is a result of the limited maturity of capabilities in the early versions of mission systems software. Although the program planned to complete developmental flight testing in January 2017, according to their Integrated Master Schedule, developed after the program was restructured in 2010, delays in issuing mature software to flight test made it clear that regression and development test points would still be needed throughout CY16.
- Cumulative SDD test point data in this report refer to the total progress towards completing development at the end of SDD.

- Limited operational testing was also conducted throughout the year to support assessments of weapon capability, deployment demonstrations, shipborne testing, and the Air Force's IOC declaration; results of these limited tests are used to support assessments throughout this report.

TEST FLIGHTS (AS OF NOVEMBER 30, 2016)

	All Testing	Flight Sciences			Mission Systems
	All Variants	F-35A	F-35B	F-35C	
2016 Planned	1,221	151	359	237	474
2016 Actual	1,362	226	386	271	479
Difference from Planned	+11.5%	+49.7%	+7.5%	+14.3%	+1.1%
Cumulative Planned	7,624	1,587	2,242	1,469	2,326
Cumulative Actual	7,853	1,697	2,318	1,479	2,359
Difference from Planned	+3.0%	+6.9%	+3.4%	+0.7%	+1.4%
Prior to CY16 Planned	6,403	1,436	1,883	1,232	1,852
Prior to CY16 Actual	6,492	1,471	1,932	1,209	1,880

TEST POINTS (AS OF NOVEMBER 30, 2016)

	All Testing	Flight Sciences						Mission Systems[1]		
		F-35A		F-35B		F-35C				
	All Variants	Block 3F Baseline	Budgeted Non-Baseline[2]	Block 3F Baseline	Budgeted Non-Baseline[2]	Block 3F Baseline	Budgeted Non-Baseline[2]	Block 3F	Budgeted Non-Baseline[2]	Other[3]
2016 Test Points Planned (by type)	8,774	1,205	159	1,876	115	1,695	146	1,189	1,534	855
2016 Test Points Accomplished (by type)	7,838	1,303	156	1,783	115	1,304	136	975	1,534	532
Difference from Planned	-10.7%	+8.1%	-1.9%	-5.0%	0.0%	-23.1%	-6.8%	-18.0%	0.0%	-37.8%
Points Added Beyond Budgeted Non-Baseline (Growth Points)	304	0		54		0		250		
Test Point Growth Percentage (Growth Points/Test Points Accomplished)	3.9%	0.0%		3.0%		0.0%		25.6%		
Total Points (by type) Accomplished in 2016[4]	8,142	1,459		1,952		1,440		3,291		
Cumulative Data										
Cumulative System Design and Development (SDD) Planned Baseline	51,060	12,225		15,994		12,604		10,237		
Cumulative SDD Actual Baseline	50,278	12,327		15,970		12,279		9,702		
Difference from Planned	-1.5%	+0.8%		-0.2%		-2.6%		-5.2%		
Est. Baseline Test Points Remaining	6,649	100		1,726		1,178		3,645		
Est. Non-Baseline Test Points Remaining	2,502	12		136		73		2,281		

1. Mission Systems Test Points for CY16 are shown only for Block 3F. Testing conducted to support Block 2B and Block 3i Mission Systems are discussed separately in the text. Cumulative numbers include all previous Mission Systems activity.
2. These points account for planned development and regression test points built into the 2016 plan; additional points are considered "growth." The total number of regression, development and discovery points completed is the sum of budgeted non-baseline test points accomplished plus points added beyond budgeted non-baseline.
3. Represents mission systems activity not directly associated with Block capability (e.g., radar cross section characterization testing, test points to validate simulator).
4. Total Points Accomplished = 2016 Baseline Accomplished + Added Points

Developmental Testing: F-35A Flight Sciences

Flight Test Activity with AF-1, AF-2, and AF-4 Test Aircraft

- F-35A flight sciences testing focused on:
  - Clearing the F-35A Block 3F flight envelope (i.e., to Mach 1.6, 700 knots, and 9.0 g) for loads, flutter, and weapons environment
  - Testing of the internal gun
  - Flight envelope clearance for external weapons required for full Block 3F weapons capability
  - Weapons separation testing of the AIM-9X missile (external only), GBU-12 bomb (external carriage added for Block 3F)
  - High energy braking, high sink rate landings, and arresting gear engagements
  - AF-4 completed all flight testing for which it had been slated, in July, and transitioned to chemical and biological testing in August

F-35A Flight Sciences Assessment

- The program planned to complete F-35A flight sciences testing by the end of October 2016; however, additional testing for weapons environment and regression of new software forced testing to continue into at least December 2016. The program was able to complete baseline test points to clear the aircraft structure for Block 3F envelope (up to 9 g, 1.6M and 700 knots), completing flutter testing on AF-2 on September 29 and loads testing on AF-1 on November 4, 2016. Through the end of November, the test team flew 50 percent more flights than planned (226 flown versus 151 planned) and accomplished 8 percent more baseline test points than planned for the year (1,303 test points accomplished versus 1,205 planned). These additional baseline test points were added by the program throughout the year and represent testing not originally budgeted for when the CY16 plans were made. The test team also flew an additional 156 test points for regression of new air vehicle software, all of which were within the budgeted non-baseline test points allocated for the year. As of the end of November the program had approximately 100 baseline test points remaining to complete F-35A flight sciences testing for Block 3F.
- The following discoveries were made during F-35A flight sciences testing:
  - Failure of the attachment joint, as indicated by the migration of the bushing in the joint, between the vertical tail and the airframe structure is occurring much earlier than planned, even with a newly designed joint developed to address shortfalls in the original design. In October 2010, the F-35A full scale durability test article, AJ-1, showed wear in the bushing of this joint after 1,784 test hours, which indicated that the joint will fall short of the 8,000 hours of service life required by the JSF contract specification. The program developed a redesigned joint and began installing them on the production line with Lot 6 aircraft, which began delivery in October 2014. Subsequently, in July 2015, when inspections showed bushing migrations and significant damage to the right and left side attachment joints in BF-3, one of the F-35B flight sciences developmental test aircraft, the joint was repaired and the bushing replaced to replicate the redesigned joint. In August, 2016, inspections of the joints in AF-2, one of the F-35A flight sciences developmental test aircraft, showed similar bushing migration requiring repair and bushing replacement in accordance with the redesign. On September 1, 2016, inspections of the vertical tail on BF-3 showed that the newly designed joint had failed, after only 250 hours of flight testing since the new joint had been installed, requiring another repair and replacement. BF-3 completed repairs and returned to flight on November 10, 2016.
  - Vibrations induced by the gun during firing are excessive and caused the 270 volts DC battery to fail. The program began qualification testing of a redesigned battery in 2015, but cracks in the casing discovered after the first series of testing required additional redesigning of the battery. Requalification of a newly designed battery has not yet occurred as of the writing of this report.
  - Limitations to the carriage and employment envelope of the AIM-120 missile above 550 knots may be required due to excessive vibrations on the missiles and bombs in the weapons bay. Analyses of flight test data and ground vibration test data are ongoing (this applies to all variants).
  - Excessive and premature wear on the hook point of the arresting gear has caused the program to consider a more robust redesign. In fact, the hook point has required replacement after only one engagement in some instances; the longest a hook point has lasted to date is five arrestments. This fails to meet the minimum service life of 15 arrestments. Additionally, failure of the hook point of the arresting gear on AF-4 occurred in July during testing of high speed engagements. However, this appears to be due to a malfunction of the Mobile Aircraft Arresting System (MAAS), which holds the arresting cable in place on both sides of the runway. The MAAS is designed to allow the arresting cable to slide across the hook upon engagement until the right and left sides are in equilibrium before the braking action to slow the aircraft takes place (this helps steer the aircraft toward the center of the runway during the engagement). For unknown reasons, only one side of the MAAS released the cable, resulting in the hook point becoming abraded by the arresting cable and failing 1.5 seconds after engagement.
  - Block 3F envelope testing required an inflight structural temperature assessment, which yielded higher than predicted air flow temperatures in the engine nacelle bay in high-speed portions of the flight envelope under high dynamic pressures. This resulted in higher than expected nacelle structural temperatures on both the F-35A and F-35C aircraft. Thermal stress analyses of the affected parts are necessary before the program can provide the full

Block 3F flight envelope for fleet release. The outcome may result in restricting fielded operational aircraft to 600 knots airspeed below 5,000 feet altitude or a structural change; this will be determined when the Services review the analyses and issue the military flight release, which certifies the operational flight envelope.

- All F-35 variants display objectionable or unacceptable flying qualities at transonic speeds, where aerodynamic forces on the aircraft are rapidly changing. Particularly, under elevated "g" conditions, when wing loading causes the effects to be more pronounced, pilots have reported the flying qualities as "unacceptable." The program adjusted control laws that govern flight control responses in an updated version of software released to flight test in March 2016. Results from flight testing of the software changes have not yet been released. Although the elevated g "dig-in" apparently affects all three variants, the program does not plan to develop any additional control law changes to mitigate these responses to aerodynamic effects in the transonic region. In operational fleet aircraft, g limit exceedances are annunciated to the pilot and, in peacetime, result in subsequent restricted maneuvering, mission termination, and a straight-in approach and landing to recover the aircraft. The aircraft is then down for some time for maintenance inspections and potential repairs. Also, the probability and long-term structural effects of the g exceedances should be assessed by the program and mitigated, if necessary.
- Foam insulation around the polyalphaolefin (PAO) coolant tubes that pass through wing and main body fuel tanks in F-35A aircraft was found to be failing after exposure to fuel. The discovery was made on a fielded production F-35A aircraft (AF-101) as it was undergoing depot-level modifications for fuel valves in August 2016. The program determined the cause was a failure of the manufacturing process with the sealant coating on the insulation designed to protect the insulation from being exposed to fuel. Instead, the sealant was permeable to fuel, permitting the insulation to absorb fuel and expand, forcing cracking and failure of the sealant coatings and eventual breakdown and flaking of the insulation. This affected a total of 57 F-35A aircraft; 42 in the production process and 15 fielded aircraft. The Air Force temporarily grounded the 15 fielded aircraft, 10 of which were designated as Initial Operational Capability aircraft. The program quickly developed inspections and implemented procedures to mitigate the insulation problems for fielded aircraft and those too far in the production line to have the fuel lines replaced with proper insulation. The procedures vary depending on whether fuel has entered the tank with the PAO lines. For aircraft in which the fuel tanks have contained fuel, the procedures involve accessing the affected fuel tanks, removing the defective insulation, installing blocking screens to prevent debris from leaving the tank (and possibly contaminating other tanks, clogging valves or affecting fuel pump operation). For the aircraft in the production line that have not yet had fuel in the tanks, the insulation will be removed from the PAO tubes, but screens will not be added to the tank. The program does not plan to re-insulate the PAO tubes, as the Block 3F avionics – which are cooled by the PAO – apparently have adequate thermal margin to tolerate the loss of insulation on the tubes. The program must ensure that deployed operating locations with high ambient temperatures – such as those in Southwest Asia – are able to provide the cooling effect necessary to prevent avionics overheat conditions, especially for heat-soaked aircraft with hot fuel tanks and during extended ground operations. The program will need to conduct another assessment for Block 4 avionics, and any new processors, to ensure the thermal margin with that hardware configuration is still adequate.
- An Air Force F-35A aircraft assigned to Luke AFB, Arizona, experienced a tailpipe fire during engine start while deployed to Mountain Home AFB, Idaho in September 2016, causing significant damage to the aircraft. The incident is under investigation.
- The program designed and fielded an electrical Engine Ice Protection System (EIPS) to protect the engine from ice damage when exposed to icing conditions during ground operations and in flight. Although it was qualified during SDD engine ground tests, no SDD aircraft have the system installed in the engine. The program fielded the system with later-lot production aircraft, but deficiencies in the system caused electrical shorting and damage to the composite blades (referred to as the Fan Inlet Variable Vanes) on the front of several engines. To prevent further damage to engines in the field, the program has disabled EIPS and is changing the technical orders to require pilots to shut down the aircraft if icing conditions are encountered on the ground. DOT&E is not aware of any corrections to the EIPS planned during SDD.
- The program completed the final weight assessment of the F-35A air vehicle for contract specification compliance in April 2015 with the weighing of AF-72, a Lot 7 aircraft. The actual empty aircraft weight was 28,999 pounds, 372 pounds below the planned not-to-exceed weight of 29,371 pounds. The actual weights of production aircraft since then have been stable, with no significant weight growth observed. Weight estimates for production Lots 10 and later indicate an expected weight growth of between 120 and 140 pounds, primarily due to new electronic warfare (EW) avionics. Weight management of the F-35A is important for meeting performance requirements and structural life expectations. The program will need to continue disciplined management of the actual aircraft weight beyond the contract specification as further discoveries during the remainder of SDD may add weight and result in performance degradation that would adversely affect operational capability.

Developmental Testing: F-35B Flight Sciences

Flight Test Activity with BF-1, BF-2, BF-3, BF-4, and BF-5 Test Aircraft

- F-35B flight sciences focused on:
  - Clearing the F-35B Block 3F flight envelope (i.e., to Mach 1.6, 630 knots, and 7.0 g)
  - High angle-of-attack testing with external stores
  - Air refueling with the British KC-30A Voyager and Air Force KC-10 aircraft
  - Mode 4 (i.e., flight with the lift fan engaged to support short takeoff and vertical landing operations) envelope expansion
  - Weapons separation testing of the AIM-9X missile (external only), GBU-12 bomb (external carriage added for Block 3F); Paveway IV bomb (internal and external) for the United Kingdom, AIM-132 missile (external only) for the United Kingdom
  - Ground gun fire testing with the F-35B gun pod; accomplished on BF-1 in July

F-35B Flight Sciences Assessment

- Through the end of November, the test team flew 8 percent more flights than planned (386 flown versus 359 planned), yet accomplished 5 percent less than the planned Block 3F baseline test points (1,783 points accomplished versus 1,876 planned). The team flew an additional 169 test points for regression of new air vehicle software, 115 of which were the budgeted non-baseline points planned for CY16 and 54 points representing growth.
- The following details discoveries in F-35B flight sciences testing:
  - Limitations to the carriage and employment envelope of the AIM-120 missile above 550 knots may be required due to excessive vibrations induced on the missiles and bombs in the weapons bay. Analyses of flight test data and ground vibration test data are ongoing (this applies to all variants).
  - All F-35 variants display objectionable or unacceptable flying qualities at transonic speeds, where aerodynamic forces on the aircraft are rapidly changing. Particularly, under elevated "g" conditions, when wing loading causes the effects to be more pronounced, pilots have reported the flying qualities as "unacceptable." The program adjusted control laws that govern flight control responses in an updated version of software released to flight test in March 2016. In the F-35B, an uncommanded aircraft g "dig-in" that exceeds design limits has been observed while performing elevated-g maneuvers in the transonic region between 0.9M and 1.05M. Significant g exceedances (up to 7.7 g; a 0.7 g exceedance) have occurred when pilots were attempting to sustain 6.5 g or greater in this region. Based on flight test data, the F-35B responses to transonic aerodynamic effects between 0.9M and 1.05M during rolling or elevated-g maneuvering cause uncommanded excursions that exceed the designed g limit as well. Although the elevated g "dig-in" apparently affects all three variants, the program does not plan to develop any additional control law changes to mitigate these responses to aerodynamic effects in the transonic region. In operational fleet aircraft, g limit exceedances are annunciated to the pilot, and in peacetime, result in subsequent restricted maneuvering, mission termination, and a straight-in approach and landing to recover the aircraft. The aircraft is then down for some time for maintenance inspections and potential repairs. Also, the probability and long-term structural effects of the g exceedances should be assessed by the program and mitigated, if necessary.
  - Horizontal tail overheating was experienced on BF-3 during loads testing while accelerating to 1.5M for a loads test point. The left horizontal inboard fairing surface reached temperatures that exceeded the design limit by a significant amount. Post-flight inspections revealed de-bonding on the trailing edge of the horizontal tail surface and heat damage was noted on the horizontal tail rear spar. Hardness checks on the rear spar were performed and were determined to be within the acceptable range. It is not yet known whether the program or the Services will impose airspeed or afterburner time restrictions in the Block 3F envelope due to horizontal tail overheating.
  - Failure of the attachment joint, as indicated by the migration of the bushing in the joint, between the vertical tail and the airframe structure, is occurring much earlier than planned, even with a newly designed joint developed to address shortfalls in the original design. In October 2010, the F-35A full scale durability test article, AJ-1, showed wear in the bushing of this joint after 1,784 test hours, which indicated that the joint will fall short of the 8,000 hours of service life required by the JSF contract specification. The program developed a redesigned joint and began installing them on the production line with Lot 6 aircraft, which began delivery in October 2014. Subsequently, in July 2015, when inspections showed bushing migrations and significant damage to the right and left side attachment joints in BF-3, one of the F-35B flight sciences developmental test aircraft, the joint was repaired and the bushing replaced, to replicate the redesigned joint. In August 2016, inspections of the joints in AF-2, one of the F-35A flight sciences developmental test aircraft, showed similar bushing migration requiring repair and bushing replacement in accordance with the redesign. On September 1, 2016, inspections of the vertical tail on BF-3 showed that the newly designed joint had failed, after only 250 hours of flight testing since the new joint had been installed, requiring another repair and replacement. BF-3 completed repairs and returned to flight on November 10, 2016.
  - An F-35B assigned to Marine Corps Air Station Beaufort, South Carolina, experienced a fire within the weapons bay during a training mission in late October 2016. The

incident, although still under investigation, resulted in a Class A mishap (involves loss of life or damage of more than $2 Million). The Marine Corps did not ground any of the training fleet as a result of the incident.
- The program designed and fielded an electrical Engine Ice Protection System (EIPS) to protect the engine and lift fan from ice damage when exposed to icing conditions during ground operations and in flight. Although it was qualified during SDD engine ground tests, no SDD aircraft have the system installed in the engine. The program fielded the system with later-lot production aircraft, but deficiencies in the system caused electrical shorting and damage to the composite blades (referred to as the Fan Inlet Variable Vanes) on the front of the several engines. To prevent further damage to engines in the field, the program has disabled EIPS and is changing the technical orders to require pilots to shut down the aircraft if icing conditions are encountered on the ground. DOT&E is not aware of any corrections to the EIPS planned during SDD.
- Weight management of the F-35B aircraft is critical to meeting the Key Performance Parameters (KPPs) in the Operational Requirements Document (ORD), including the Vertical Landing Bring-Back (VLBB) requirement, which will be evaluated during IOT&E. This KPP requires the F-35B to be able to fly an operationally representative profile and recover to the ship with the necessary fuel and balance of unexpended weapons (two 1,000-pound bombs and two AIM-120 missiles) to safely conduct a vertical landing.
  - The program completed the final weight assessment of the F-35B air vehicle for contract specification compliance in May 2015 with the weighing of BF-44, a Lot 7 production aircraft. Actual empty aircraft weight was 32,442 pounds, only 135 pounds below the planned not-to-exceed weight of 32,577 pounds and 307 pounds (less than 1 percent) below the objective VLBB not-to-exceed weight of 32,749 pounds.
  - The actual weights of production aircraft through Lot 8 have increased slightly, with the latest Lot 8 aircraft weighing approximately 30 pounds heavier than BF-44. Weight estimates for Lot 10 aircraft and later project weight growth of an additional 90 pounds, primarily due to additional EW equipment.
  - Known modifications to the 14 Lot 2 through 4 F-35B aircraft, required to bring those aircraft to the Block 3F configuration, are expected to potentially add an additional 350 pounds, which will push their weight above the objective not-to-exceed weight to meet the VLBB KPP. This KPP will be evaluated during IOT&E with an F-35B OT aircraft.
  - Estimates for FoM weight growth include an additional 250 pounds, which will exceed the vertical landing structural limit not-to-exceed weight of 33,029 pounds for the Lot 2 through Lot 4 aircraft. This additional weight may prevent these aircraft from being upgraded to the Block 4 configuration.

Developmental Testing: F-35C Flight Sciences

Flight Test Activity with CF-1, CF-2, CF-3, and CF-5 Test Aircraft

- F-35C flight sciences focused on:
  - Clearing the F-35C Block 3F flight envelope (i.e., to Mach 1.6, 700 knots, and 7.5 g)
  - Air refueling with F/A-18, KC-10, and KC-135 aircraft
  - Weapons separation testing of the AIM-9X missile (external only), Joint Standoff Weapon (JSOW, internal only), GBU-12 bomb (external carriage added for Block 3F)
  - Shore-based ship suitability testing with external stores, in preparation for shipborne trials that were conducted in August
  - High angle-of-attack testing with external stores
  - Testing of the Joint Precision Approach and Landing System (JPALS)
  - Ground gun fire testing with the F-35C gun pod; accomplished on CF-3 in November

F-35C Flight Sciences Assessment

- Through the end of November, the test team flew 14 percent more than planned flights (271 flown versus 237 planned), but accomplished 23 percent less than the planned Block 3F baseline test points (1,304 points accomplished versus 1,695 planned). The team flew an additional 136 test points for regression of new software, all of which were accounted for in the budgeted non-baseline points planned for the year.
- The following details discoveries in F-35C flight sciences testing:
  - Flight testing of structural loads with the AIM-9X air-to-air missile, which will be carried on external pylons outboard of the wing fold in the F-35C, shows exceedances above the wing structural design limit during flight in regions of aircraft buffet (increased angle-of-attack) and during landings. To address these deficiencies, the program is developing a more robust outer wing design, which is scheduled for flight testing in early CY17. Without the redesigned outer wing structure, the F-35C will have a restricted flight envelope for missile carriage and employment, which will be detrimental to maneuvering, close-in engagements.
  - Limitations to the carriage and employment envelope of the AIM-120 missile above 550 knots may be required due to excessive vibrations induced on the missiles and bombs due to the acoustics in the weapons bay. Analyses of flight test data and ground vibration test data are ongoing (this applies to all variants).
  - All F-35 variants display objectionable or unacceptable flying qualities at transonic speeds, where aerodynamic forces on the aircraft are rapidly changing. Particularly, under elevated "g" conditions, when wing loading causes the effects to be more pronounced, pilots have reported the flying qualities as "unacceptable." The program adjusted control laws that govern flight control responses in an updated version of software released to flight test in March 2016. In the F-35C, like the other variants, an

uncommanded aircraft g "dig-in" that exceeds design limits has been observed while performing testing of elevated-g maneuvers in the transonic region of the flight envelope. While attempting to sustain a maximum g (7.5g) turn, an F-35C test aircraft experienced 8.2 g – an exceedance of 0.7 g. The program does not plan to develop any additional control law changes to address the flying quality. Similar to the other variants, an over-g condition requires the pilot to terminate the mission (in peacetime) and recover the aircraft with a straight-in approach and landing with minimal maneuvering. The aircraft is then down for some time for maintenance inspections and potential repairs. Also, the probability and long-term structural effects of the g exceedances should be assessed by the program and mitigated, if necessary.

- Weapons environment testing showed that the aircraft experienced transient rolling conditions while asymmetrically opening and closing the weapon bay doors (WBD). The flight control laws were designed to compensate for the doors opening and closing asymmetrically. The program corrected the on-board aerodynamic models in two vehicle systems software updates (versions R31.1 and R35.1) to reduce the roll transients. These corrections resolved the transients for the subsonic and transonic flight regimes, but not for supersonic regimes. The operational impact of these transients will be assessed during IOT&E.
- Block 3F envelope testing required an inflight structural temperature assessment, which yielded higher than predicted air flow temperatures in the engine nacelle bay in high-speed portions of the flight envelope under high dynamic pressures. This resulted in higher nacelle structural temperatures on both the F-35A and F-35C aircraft. Thermal stress analyses of the affected parts are necessary before the program can provide the full Block 3F flight envelope for fleet release. The outcome may result in restricting fielded operational aircraft to 600 knots airspeed below 5,000 feet altitude, or a structural change; this will be determined when the Services review the analyses and issue the military flight releases, which will certify the operational flight envelope.
- As reported in previous DOT&E Annual Reports, the F-35C experiences buffet and transonic roll off (TRO), an uncommanded roll, at transonic Mach numbers and elevated angles of attack. It is caused by the impact of airflow separating from the leading edge of the wing that "buffets" aft areas of the wing and aircraft during basic fighter maneuvering. The TRO and buffet occur in areas of the maneuvering envelope that cannot be sustained for long periods of time, as energy depletes quickly and airspeed transitions out of the flight region where these conditions manifest. However fleeting, these areas of the envelope are used for critical maneuvers. Operational testing of the F-35C during IOT&E will assess the effect of TRO and buffet on overall mission effectiveness.
- Due to the stiffness of the landing gear struts, particularly the nose gear, taxiing in the F-35C results in excessive jarring of the aircraft and often requires pilots to stop taxiing if they need to make changes using the touchscreens on the cockpit displays or to write information on their kneeboard. Currently, the program has no plans to correct the deficiency of excessive jarring during F-35C taxi operations.
- Excessive vertical oscillations during catapult launches make the F-35C operationally unsuitable for carrier operations, according to fleet pilots who conducted training onboard USS *George Washington* during the latest set of ship trials. Although numerous deficiencies have been written against the F-35C catapult launch – starting with the initial set of F-35C ship trials (DT-I) in November 2014 – the deficiencies were considered acceptable for continuing developmental testing. Fleet pilots reported that the oscillations were so severe that they could not read flight critical data, an unacceptable and unsafe situation during a critical phase of flight. Most of the pilots locked their harness during the catapult shot which made emergency switches hard to reach, again creating, in their opinion, an unacceptable and unsafe situation. The U.S. Navy has informed the Program Office that it considers this deficiency to be a "must fix" deficiency. The program should address the deficiency of excessive vertical oscillations during catapult launches within SDD to ensure catapult operations can be conducted safely during IOT&E and during operational carrier deployments.
- Overheating of the Electro-Hydraulic Actuator System (EHAS) occurs under normal maneuvering in the F-35C. The EHAS actuators move the flight surfaces and are cooled by airflow across the control surfaces. Pilots are alerted in the cockpit of an overheat condition and must then minimize maneuvering and attempt to cool the EHAS by climbing, if practical, to an altitude with lower temperatures to enhance cooling. Recovery and landing must be completed as soon as possible, terminating the mission.
- The program designed and fielded an electrical Engine Ice Protection System (EIPS) to protect the engine from ice damage when exposed to icing conditions during ground operations and in flight. Although it was qualified during SDD engine ground tests, no SDD aircraft have the system installed in the engine. The program fielded the system with later-lot production aircraft, but deficiencies in the system have caused electrical shorting and damage to the composite blades (referred to as the Fan Inlet Variable Vanes) on the front of the engine. To prevent further damage to engines in the field, the program has disabled EIPS and is changing the technical orders to require pilots to shut down the aircraft if icing conditions are encountered on the ground. DOT&E is not aware of any corrections to the EIPS planned during SDD.

- Weight management of the F-35C is important for meeting air vehicle performance requirements, including the KPP for recovery approach speed to the aircraft carrier, and structural life expectations. The program completed the final weight assessment of the F-35C air vehicle for contract specification compliance in May 2016 with the weighing of CF-28, a Lot 8 aircraft. The actual empty aircraft weight was 34,581 pounds, 287 pounds below the planned not-to-exceed weight of 34,868 pounds. The weights of the other three Lot 8 production aircraft have been consistent with that of CF-28. Weight estimates for production Lots 11 and later indicate an expected weight growth of approximately 160 pounds. The program will need to continue rigorous management of the actual aircraft weight through the balance of SDD to avoid performance degradation that would affect operational capability.

Developmental Testing: Mission Systems

- Mission systems are developed, tested, and fielded in incremental blocks of capability.
  - Block 1. The program designated Block 1 for initial training capability in two increments: Block 1A for Lot 2 (12 aircraft) and Block 1B for Lot 3 aircraft (17 aircraft). No combat capability was available in either Block 1 increment. The Services have upgraded all of these aircraft to the Block 2B configuration through a series of modifications and retrofits. Additional modifications will be required to configure these aircraft in the Block 3F configuration.
  - Block 2A. The program designated Block 2A for advanced training capability and delivered aircraft in production Lots 4 and 5 in this configuration. No combat capability was available in Block 2A. The Services accepted 62 aircraft in the Block 2A configuration (32 F-35A aircraft in the Air Force, 19 F-35B aircraft in the Marine Corps, and 11 F-35C aircraft in the Navy). Similar to the Block 1A and Block 1B aircraft, the Services have upgraded all of the Block 2A aircraft to the Block 2B configuration with modifications and retrofits, although fewer modifications were required. Additional modifications will be required to fully configure these aircraft in the Block 3F configuration.
  - Block 2B. The program designated Block 2B for initial, limited combat capability with selected internal weapons (AIM-120C, GBU-31/32 JDAM, and GBU-12). This block is not associated with the delivery of any lot of production aircraft, but with an upgrade of mission systems software capability for aircraft delivered through Lot 5 in earlier Block configurations. Block 2B is the software that the Marine Corps accepted for the F-35B IOC configuration. Corrections to some deficiencies identified during Block 2B and Block 3i mission systems testing have been included in the latest production release of Block 2B software – version 2BR5.3 – fielded in May 2016 after airworthiness testing in April. The Services began converting aircraft from these earlier production lots to the Block 3i configuration by replacing the older Technical Refresh 1 (TR1) integrated core processor with newer Technical Refresh 2 (TR2) processors this year. As of the end of November, 1 F-35A (AF-31) and 1 F-35B (BF-19) had completed the TR2 modifications, both of which are instrumented operational test aircraft. The Marine Corps declared IOC with Block 2B-capable aircraft in July 2015.
  - Block 3i. The program designated Block 3i for delivery of aircraft in production Lots 6 through 8, as these aircraft include a set of upgraded TR2 integrated core processors. The program delivered Lot 6 aircraft with a Block 3i version that included capabilities equivalent to Block 2A in Lot 5. Lot 7 aircraft were delivered with capabilities equivalent to Block 2B, as are Lot 8 aircraft currently. Block 3i software began flight testing in May 2014 and completed baseline testing in October 2015, eight months later than planned in the Integrated Master Schedule (IMS). Because of software immaturity and instability during startup and in flight, the program paused flight testing of Block 3F software in February 2016 (software version 3FR5) and returned to Block 3i development and flight testing to address poor mission systems stability. After completing flight testing in April of another build of Block 3i software, version 3iR6.21, that version was fielded to the operational units with improved stability performance, which was similar to that seen in the latest build of Block 2B software. By the end of November, the program had delivered 51 F-35A aircraft to the Air Force, 17 F-35B aircraft to the Marine Corps, and 13 F-35C to the Navy in the Block 3i configuration in Lots 6, 7 and 8. The Air Force declared IOC with Block 3i-capable aircraft in August 2016.
  - Block 3F. The program designated Block 3F as the full SDD warfighting capability for production Lot 9 and later. Block 3F expands the flight envelope for all variants and includes additional weapons, external carriage of weapons, and the gun. Flight testing with Block 3F software on the F-35 test aircraft first began in March 2015. Flight testing of Block 3F mission systems software, version 3FR5, was paused in February 2016 when the program discovered that it was too unstable for productive flight testing. The program elected to reload a previous version of Block 3F software – version 3FR4 – on the mission systems flight test aircraft, to allow limited testing to proceed. After improving the flight stability of the Block 3i software, the program applied the corrections to deficiencies causing instabilities to the Block 3FR5 software and delivered another version to flight test – version 3FR5.02 – in March, to continue Block 3F testing. The program restarted Block 3F testing in earnest in May with Block 3FR5.03 and released several more Quick Reaction Cycle (QRC) versions, Blocks 3FR5.04 through 3FR5.07, through November 2016 in attempts to quickly address key deficiencies that were blocking test points. The program delivered the final planned version of Block 3F software –

3FR6 – to flight testing in December 2016. The program will then determine, with testing in early 2017, if additional QRC patches will be adequate to meet specifications, or if another full release of Block 3F software (e.g., 3FR7) will be required. Of note, all of the aircraft from earlier production lots, i.e., Lots 2 through 5 will need to be modified, including structural modifications and the installation of TR2 processors, to have full Block 3F capabilities. The program plans to begin delivering Lot 9 aircraft in early CY17. The Program Office has agreed to allow the initial Lot 9 aircraft to be delivered with Block 3i software. These provisional acceptances may continue until August 2017, when the program plans to have Block 3FP8 – the first version of Block 3F production software – for delivery of the remainder of Lot 9 and later aircraft.

- Block 4. The program has designated the first release of added capabilities following completion of SDD as Block 4, with four distinct increments (Blocks 4.1, 4.2, 4.3, and 4.4). Current program schedules plan for testing of Block 4.1 to begin at the end of CY19 with subsequent increments following at 2-year intervals. Hardware upgrades are planned in Blocks 4.2 and 4.4, and will include the next upgrade in processors with open-architecture Technical Refresh 3 (TR3) processors. Production cut-in for initial Block 4.1 capabilities is planned with Lot 13, beginning delivery in 2021, and Lot 15 for Block 4.2. The post-SDD development program is referred to as Follow-on Modernization (FoM). However, for reasons discussed elsewhere in this report, the program's initial FoM plan is not executable and is being re-planned by the program and stakeholders.

Flight Test Activity with AF-3, AF-6, AF-7, BF-4, BF-5, BF-17, BF-18, CF-3, CF-5, and CF-8 Flight Test Aircraft and Software Development Progress

- Mission systems testing focused on:
  - Attempting to resolve software stability problems with Block 2B and Block 3i mission systems
  - Block 3F mission systems development and testing
  - Initial integration testing of the U.S. Navy Joint Standoff Weapon, version C1 (JSOW-C1)
  - Completing weapons separation testing for the Small Diameter Bomb (SDB) version I (SDB-I), which requires mission systems-capable aircraft for interfacing with the SDB
  - Weapons integration and testing of the United Kingdom Paveway IV bomb and Advanced Short-Range Air-to-Air Missile (ASRAAM); determining root cause and options to fix ASRAAM integration deficiencies
  - On-Board Inert Gas Generation System (OBIGGS) testing on CF-8, the only F-35C test aircraft modified with the necessary hardware to complete testing
  - Regression testing of Block 2B software on operational test aircraft (AF-21, AF-23, BF-16 and BF-20), since the developmental test aircraft had all already been converted to the Block 3i or Block 3F configuration
  - Joint Precision Approach and Landing System (JPALS) testing with CF-5
  - Testing of the Gen III Helmet Mounted Display System (HMDS) illumination settings during the third F-35C developmental test period at sea, designed to correct excessive "green glow" during night operations onboard the carrier
  - The six mission systems developmental flight test aircraft assigned to the Edwards AFB test center flew an average rate of 6.9 flights per aircraft, per month in CY16 through November, slightly above the planned rate of 6.7 for the year, and flew slightly more than the planned number of flights (479 flights accomplished versus 474 planned).

Mission Systems Assessment

- Block 2B
  - Although the program completed Block 2B mission systems testing in 2015 and provided a fleet release version of the software to the fielded units, deficiencies remained and were carried forward into Block 3i. This schedule-driven decision to pass deficiencies forward had consequences. The many deficiencies, including instabilities in both Block 3i and Block 3F mission systems software, led the program to return to Block 3i development to make corrections. When the revised Block 3i software, Block 3iR6.21, demonstrated improved inflight stability, the program developed and tested another version of Block 2B software – version 2BS5.3 – with the corrections to the stability deficiencies included. This version was released to fielded units in May 2016 for the F-35A and F-35B, and in August 2016 for the F-35C; the program expects to complete retrofit of all fielded aircraft in the Block 2B configuration with the Block 2BS5.3 software by the end of January 2017.
  - Because the test center aircraft had all been upgraded to the Block 3i/3F configuration (i.e., with the newer TR2 processors), flight testing of the Block 2BS5.3 software occurred on OT aircraft assigned to the OT squadron at Edwards AFB, California.
- Block 3i
  - Block 3i began with the schedule-driven decision to rehost the immature Block 2B software and capabilities into new TR2 avionics processors. Because of the extreme overlap of development and production, combined with delays in software development, the program was forced to create a Block 3i capability to support delivery of Lot 6 and later aircraft, as they were being delivered with the new processors. Although the program originally intended that Block 3i would not inherit technical problems from earlier blocks, this is what occurred, resulting in severe problems with Blocks 3i and 3F software that needed to be addressed, affecting both Block 2B and Block 3i fielded aircraft, and stalling the progress of mission systems testing early in CY16.
  - When Block 3i developmental flight testing began in May 2014, six months later than planned in the program's

Integrated Master Schedule (IMS), the combination of rehosted, immature software and new processors resulted in severe avionics stability problems that were significantly worse than those in Block 2B. Continued delays in completing Block 2B software development and testing in support of the Marine Corps IOC, which was a priority over Block 3i development for the program and the test centers, combined with the severe stability problems with the early versions of Block 3i software, caused several pauses in early Block 3i flight testing. Block 3i flight testing resumed again in March 2015 and was considered to be complete in October 2015, eight months later than planned in the IMS. Despite the continued problems with avionics stability, sensor fusion, and other inherited issues from Block 2B, the program terminated Block 3i developmental flight testing in October 2015, and released Block 3i software to the fielded units. This decision was made in an attempt to meet the program's unrealistic schedule for completing development and flight testing of Block 3F mission systems.

- The program created an initial version of Block 3F software by adding the final required capabilities and weapons to the problematic Block 3i software. However, productive and efficient flight testing was not possible due to inherited instabilities and other deficiencies. The Air Force insisted on fixes for seven (five identified in 2014 and two more in 2015) of the most severe deficiencies inherited from Block 2B as a prerequisite to use the final Block 3i capability in the Air Force IOC aircraft. Consequently, in February 2016, the program decided to return to Block 3i development and testing in another attempt to fix key unresolved software deficiencies, including the avionics instabilities troubling both Block 3i and Block 3F. A new version of mission systems software, Block 3iR6.21, was quickly developed and tested, and showed improvement to several of the "must fix" deficiencies identified by the Air Force and the inflight stability problems, so it was released to the fielded aircraft in late May 2016. Data collected on start-up and inflight stability of the Block 3iR6.21 mission systems software showed that both have improved over earlier versions of Block 3i, and are approximately equivalent to the final version of Block 2B software. Based on flights conducted with the production software through the end of October 2016, the Air Force reported that, of the seven "must fix" deficiencies, five had been corrected, one was partially corrected, but needed full Block 3F set of capabilities to ensure full implementation, and one – associated with extended post-mission download times from the aircraft's portable memory device (PMD) – was awaiting fielding of an upgraded ground data receptacle (see more detail in the ALIS section below).

• Block 3F
  - Block 3F flight testing began in March 2015, six months later than the date planned in the IMS.
  - The emphasis on, and return to, Block 3i testing in March and April 2016 contributed in part to the program's inability to progress with Block 3F flight testing at the planned rate. As of the end of November, a total of 975 Block 3F baseline test points had been completed in CY16, compared to 1,189 planned (82 percent of planned). An additional 1,784 development and regression points were flown, 1,534 of which were accounted for in the budgeted non-baseline points for the year and 250 representing growth.
  - The lag in completing baseline test points – which are used to verify capability – is also due to the program delivering Block 3F software to flight test that was not mature enough to meet specification compliance, or because deficiencies prevent the specification from being met. In an attempt to address the deficiencies and the lack of maturity in the software, the program began developing and delivering QRC versions of software to flight test. These software versions are built, lab tested, and delivered to flight test on a shorter timeline than the originally planned series of software versions for Block 3F.
  - Delays in starting Block 3F testing, pausing to redo Block 3i work, and the immaturity of the Block 3F software delivered to flight test have all contributed to the program being well behind the plan to complete Block 3F flight testing by the end of July 2017, the forecasted completion date according to the program's most recent Mission Systems Software and Capability Release Schedule. Instead, DOT&E estimates the program will likely not finish Block 3F development and flight testing prior to July 2018, based on the following:
    ▪ Continuing a 6.5 test point per flight accomplishment rate, which is the CY16 rate observed through the end of November.
    ▪ Continuing a flight rate of 6.9 flights per aircraft per month, as was achieved through the end of November.
    ▪ Completing all of the baseline test points (3,645 remaining as of the end of November) and experiencing a regression, development and discovery test point work load of 63 percent (historical average, but well below the rate of 83 percent experienced in CY16 through November).
  - The program plans to truncate the planned testing by eliminating test points, instead using alternative test points or old data, in order to meet schedule deadlines with the expectation of finishing SDD, getting to IOT&E, and starting full-rate production. While this approach may provide a quick sampling assessment of Block 3F capabilities, there are substantial risks. The multiple recent software versions for flight test may prevent the program from using data from older versions of software to count for baseline test point deletions because it may no longer be representative of Block 3F. Limited availability and high cost of range periods, combined with high re-fly rates for test missions completed on the Western Test

Range, make it difficult for the program to efficiently conduct this testing. Finally, the most complex capabilities in Block 3F have only recently reached the level of maturity to allow them to be tested, and they are also some of the most difficult test points to execute (i.e., full Block 3F capabilities and flight envelope). Such a risky course of action, if not properly executed with applicable data, sufficient analytical rigor and statistical confidence, would likely result in failures in IOT&E causing the need for additional follow-on operational testing, and, most importantly, deliver Block 3F to the field with severe shortfalls in capability – capability that the Department must have if the F-35 is ever needed in combat against current threats. In fact, the plan to eliminate or replace test points is at a point in the development program where the most difficult, yet some of the most important capabilities, have just started to reach maturity to begin flight testing. The program should complete testing of all necessary Block 3F baseline test points, as defined in the Joint Test Plans; if the program attempts to use test data from previous testing or added complex test points to sign off some of these test points, the program must ensure the data are applicable and provide sufficient statistical confidence prior to deleting any underlying build-up test points. Additionally, the program should consider adding another full version of Block 3F software to develop and deliver to flight test in order to address more deficiencies.

- Deficiencies in performance and significant operational shortfalls must be resolved if the program is to deliver the expected full Block 3F capability by the end of SDD. Based on operational test pilot observations of developmental test missions flown in June and July 2016, an assessment of the operational utility of Block 3FR5.03 software to support planned IOT&E missions, including Close Air Support, Suppression/Destruction of Enemy Air Defenses, Offensive and Defense Counter-Air, Air Interdiction, and Surface Warfare, rated each of the mission areas "red" and unacceptable overall. Additionally, the JOTT provided an assessment of the Block 3F capabilities, based on observing and assisting with F-35 developmental testing with Block 3FR5.05 software, which began flight testing in August. The team's assessment made top-level, initial predictions of expected IOT&E results of the F-35 for each of the mission areas. The team predicted severe or substantial operational impacts across all the planned IOT&E missions, similar to the list of missions above, due to shortfalls and deficiencies, with the exception of the Reconnaissance mission area, which predicted minimal operational impact. The program should ensure adequate resources remain available (personnel, labs, flight test aircraft) through the completion of IOT&E to develop, test and verify corrections to deficiencies identified during flight testing that may cause operational mission failures during IOT&E or in combat.
- The program plans to provide full Block 3F capability, as defined in the TEMP, with the first Lot 10 aircraft delivery in January 2018. In fact, as required by the National Defense Authorization Act (NDAA) for FY16, the Secretary of the Air Force certified to Congress in September 2016 that these aircraft will have full combat capability, as determined as of the date of the enactment of the NDAA, with Block 3F hardware, software, and weapons carriage. However, for many reasons, it is clear that the Lot 10 aircraft will not initially have full Block 3F capability. These reasons include, but are not limited to, the following:
  - Envelope limitations will likely restrict carriage and employment of the AIM-120 missile and bombs well into 2018, if not later.
  - The full set of geographically specific area of responsibility MDLs will not be complete, i.e., developed, tested and verified, until 2019, at the soonest, due to the program's failure to provide the necessary equipment and software tools for the USRL.
  - Even after they are delivered, the initial set of MDLs will not be tested and optimized to deal with the full set of threats present in operational test, let alone in actual combat, which is part of full combat capability.
  - The program currently has more than 270 Block 3F unresolved high-priority (Priority 1 and Priority 2, out of a 4-priority categorization) performance deficiencies, the majority of which cannot be addressed and verified prior to the Lot 10 aircraft deliveries; less than half of these deficiencies were being actively worked in Block 3F.
  - The program currently has 17 known and acknowledged failures to meet the contract specification requirements, all of which the program is reportedly planning to get relief from the SDD contract due to lack of time and funding.
  - Dozens of contract specification requirements are projected to be open into FY18; these shortfalls in meeting the contract specifications will translate into limitations or reductions to full Block 3F capability.
  - Estimates to complete Block 3F mission systems that extend into the summer of 2018 have been put forth not just from DOT&E, but also from other independent Department agencies (e.g., CAPE), affirming that delivery of full capability in January 2018 will be nearly impossible to achieve, unless testing is prematurely terminated, which would increase the likelihood that the full Block 3F capabilities will not be adequately tested and priority deficiencies fixed.
  - Deficiencies continue to be discovered at a rate of about 20 per month, and many more will undoubtedly be discovered before and during IOT&E.
  - ALIS version 3.0, which is necessary to provide full combat capability, will not be fielded until mid-2018, and a number of capabilities that had previously been designated as required for ALIS 3.0 are now being

deferred to later versions of ALIS (i.e., after summer of 2018).
  - The Department has chosen to not fund the program to the CAPE estimate that the completion of Block 3F mission systems testing will last until mid-2018, a time span which is much later than, and at a cost that is at least double, the Program Office's latest unrealistic estimate to complete SDD. This guarantees the program will attempt a premature resource- and schedule-driven shutdown of mission systems testing which will increase the risk of mission failures during IOT&E and, more importantly, if the F-35 is used in combat.
  - Finally, rigorous operational testing in IOT&E, which provides the most credible means to predict combat performance in advance of actual combat, will not be completed until at best the end of 2019 – and more likely later.

Assessment of Block 2B and 3i "Initial Warfighting" Fielded Capability

- Using aircraft in the Block 2B configuration, both the Air Force, with the F-35A, and the Marine Corps, with the F-35B, have flown simulated combat missions during training or in support of training exercises. These training missions have highlighted numerous shortfalls in Block 2B capability.
  - Unlike legacy aircraft, Block 2B aircraft will need to make substantial use of voice communications to receive targeting information and clearance to conduct an attack during Close Air Support (CAS) missions due to the combined effects of digital data communications deficiencies, lack of infrared pointer capability, limited ability to detect infrared pointer indications from a controller (which may be improved in the Generation III Helmet Mounted Display System (Gen III HDMS)), and inability to confirm coordinates loaded to GPS-aided weapons. Each of these shortfalls limit effectiveness and increase the risk of fratricide in combat.
  - Many pilots assess and report that the Electro-Optical Targeting System (EOTS) on the F-35 is inferior to those currently on legacy systems, in terms of providing the pilot with an ability to discern target features and identify targets at tactically useful ranges, along with maintaining target identification and laser designation throughout the attack. Environmental effects, such as high humidity, often forced pilots to fly closer to the target than desired in order to discern target features and then engage for weapon employment, much closer than needed with legacy systems, potentially alerting the enemy, exposing the F-35 to threats around the target area or requiring delays to regain adequate spacing to set up an attack. However, due to design limitations, there are no significant improvements to EOTS planned for Block 3F.
  - When F-35 aircraft are employed at night in combat, pilots are restricted from using the current limited night vision camera in the Generation II helmet with Block 2B aircraft. This restriction does not apply to pilots equipped with the Generation III helmet, which is fielded with the Block 3i aircraft. In general, if used in combat, pilots flying Block 2B aircraft would operate much like early fourth generation aircraft using cockpit panel displays, with the Distributed Aperture System providing limited situational awareness of the horizon, and heads-up display symbology projected on the helmet.
- Because Block 3i is an interim capability based on Block 2B, it inherited numerous limitations that will reduce operational effectiveness and require workarounds if F-35 in the Block 3i configuration are used in combat. The Air Force conducted an IOC Readiness Assessment (IRA), using F-35A aircraft with four different versions of Block 3i mission systems software. Based on observations from fielded units and from the Air Force's IRA, the following mission areas will be affected by limitations, which may affect overall effectiveness:
  - Close Air Support (CAS). In many ways, the F-35 in the Block 3i configuration does not yet demonstrate CAS capabilities equivalent to those of fourth generation aircraft. The F-35A in the Block 3i configuration has numerous limitations that make it less effective overall in the CAS mission role than most currently fielded fighter aircraft like the F-15E, F-16, F-18 and A-10 in a permissive or low-threat environment, which is where CAS is normally conducted. These limitations, consistent with observations made by the Air Force in its IRA report, include:
    - The limited weapons load of two bombs (along with two missiles for self-defense) constrains the effectiveness of the Block 3i F-35 for many CAS missions. Compared to a legacy fighter with multiple weapons on racks, and multiple weapons types per aircraft, the limited Block 3i load means that only a limited number and type of targets can be effectively attacked.
    - No gun capability. An aircraft-mounted gun is a key weapon for some CAS scenarios when a bomb cannot be used due to collateral damage concerns or when the enemy is "dangerously close" to friendly troops. The gun can also be an effective weapon for attacking moving targets. However, even though an internal gun is installed in the Block 3i F-35A, it cannot be used until significant modifications to both the gun system and aircraft are completed, and a version of Block 3F software is tested and delivered to fielded aircraft. Gun weapons delivery accuracy (WDA) testing, aimed by the HMDS, with the required modifications and software, has slipped from September 2016 to early 2017. Initial build-up testing for the gun WDA was being planned for December 2016 at the time of writing this report.
    - Limited capability to engage moving targets. Even though the Block 3i F-35A does not have a functioning gun, it can carry the GBU-12 laser guided bomb which has limited moving target capability. However, Block 3i (and Block 3F because it is currently not planned to be addressed) does not have an automated targeting

function with lead-laser guidance (i.e., automatically computing and positioning the laser spot proportionately in front of the moving target to increase the likelihood of hitting the target) to engage moving targets with the GBU-12, like most legacy aircraft have that currently fly CAS missions. Instead, F-35 pilots can only use basic rules-of-thumb when attempting to engage moving targets with the GBU-12, resulting in very limited effectiveness. Also, limitations with cockpit controls and displays have caused the pilots to primarily use two-ship "buddy lasing" for GBU-12 employment, which is not always possible during extended CAS engagements when one of the aircraft has to leave to refuel on a tanker. To meet the ORD requirement for engaging moving targets, the Air Force is considering integrating the GBU-49, a fielded weapon that has similar size, weight and interfaces as the GBU-12, or a similar weapon that does not require lead-laser guidance, in Block 3F. Otherwise, the program plans to develop and field lead-laser guidance in Block 4.2, which would be delivered in CY22, at the earliest. However, because of the similarities, the GBU-49 could be quickly integrated with Block 3F to provide a robust moving target capability for the F-35 much earlier.

▪ Voice communications are sometimes required to validate digital communications. Problems with Variable Message Format (VMF) and Link-16 datalink messaging – including dropped or hidden information or incorrect formats – sometimes require pilots to use workarounds by validating or "reading back" information over the radio that prevent them from conducting digital (only) CAS, a capability that is common in most legacy CAS aircraft. Recent use of VMF digital communications during weapons demonstration events by the operational test teams has been more successful; however, data analyses are ongoing.

▪ Limited night vision capability. Although Lot 7 and later aircraft are fielded with the Gen III HMDS, which has shown improvement to the deficiencies with the earlier Gen II HMDS, limitations with night vision capability remain. Pilots using the Gen III helmet for night operations report that visual acuity is still less than that of the night vision goggles used in legacy aircraft, which makes identification of targets and detecting markers more difficult, if not impossible. Also, "green glow" – a condition where light leakage around the edge of the display during low-light conditions makes reading the projected information difficult – is improved over the Gen II HMDS, but is still a concern during low ambient illumination conditions. The program currently has two open "Category 1 High" deficiency reports for "green glow," with the most significant safety concerns pertaining to nighttime carrier operations.

▪ Lack of target marking capability – a key capability for both Forward Air Controller-Airborne (FAC-A) and CAS missions. Legacy CAS platforms can mark targets with rockets, flares, and/or infrared (IR) pointers, none of which are currently available on the F-35. The F-35 has a laser designator as part of its Electro-Optical Targeting System (EOTS), but the laser is used for targeting from ownship when using the GBU-12 laser guided bomb or to "buddy-guide" a weapon from another aircraft. This limitation is not planned to be fixed during SDD.

- Other mission areas. In addition to the Block 3i limitations listed above that affect the CAS mission area, the following inherent Block 3i limitations will also affect the capability of the F-35 in other mission areas:
  ▪ Poor ability to accurately locate (i.e., determine geographic location with precision needed for weapons employment) and identify threat emitters.
  ▪ No standoff weapon. With only direct attack bombs, the F-35 in the Block 3i configuration will be forced to fly much closer to engage ground targets and, depending on the threat level of enemy air defenses and acceptable mission risk, it may be limited to engaging ground targets that are defended by only short-range air defenses, or by none at all.
  ▪ The limited weapons loadout of the Block 3i F-35 makes effective attack of many expected types of targets in a typical theater a challenge. For example, unlike legacy aircraft, the Block 3i F-35 has no mixed weapons load capability, which limits flexibility to attack targets with appropriately matched weapons. Block 3i F-35 aircraft can only employ two internally carried bombs, and although internal carriage reduces the susceptibility of the F-35 relative to legacy aircraft, by virtue of the low observability it provides, it does not provide the ability to attack more than one or two targets.
  ▪ Pilots report that inadequacies in Pilot Vehicle Interfaces (PVI) in general, and deficiencies in the Tactical Situation Display (TSD) in particular, which displays the results of sensor fusion and is designed to provide increased situation awareness, continue to degrade battlespace awareness and increase pilot workload. Workarounds to these deficiencies are time-consuming for the pilot and detract from efficient and effective mission execution.
- Block 3i has significant deficiencies that must still be addressed, despite the additional software release to the field, Block 3iP6.21, in May 2016. In addition to the limitations listed above, Block 3i also has hundreds of other deficiencies, the most significant of which must be fixed in Block 3F to realize the full warfighting capability required of the F-35. These deficiencies include, but are not limited to, the following:
  ▪ Avionics sensor fusion performance is still unacceptable.
    » Air tracks often split erroneously or multiple false tracks on a single target are created when all sensors contribute to the fusion solution. The workaround during early developmental testing was to turn off

some of the sensors to ensure multiple tracks did not form, which is unacceptable for combat and violates the basic principle of fusing contributions from multiple sensors into an accurate track and clear display to gain situational awareness and to identify and engage enemy targets.
 - » Similarly, multiple false ground tracks often are displayed when only one threat emitter is operating. In addition, tracks that "time out" and drop from the display cannot be recalled, which can cause pilots to lose tactical battlefield awareness on enemy air defense radars that turn on only intermittently, as is typical of missile engagement radars.
 - » Sharing erroneous tracks over the Multifunction Advanced Data Link (MADL) between aircraft in the F-35 formation multiplies the problems described above.
 - » The Air Force IOC Readiness Assessment (IRA) report also identified deficiencies with fusion in Block 3i.
- ▪ Electronic warfare (EW) capabilities, including electronic attack (EA), are inconsistent and, in some cases, not effective against required threats.
 - » Although the details of the deficiencies are classified, effective EW capabilities are vital to enable the F-35 to conduct Suppression/Destruction of Enemy Air Defenses (SEAD/DEAD) and other missions against fielded threats.
 - » The Air Force IRA report also identified significant EW deficiencies in Block 3i.
- ▪ Datalinks do not work properly. Messages sent across the MADL are often dropped or pass inaccurate offboard inter-flight fusion tracks based on false or split air tracks and inaccurate ground target identification and positions.
- ▪ Reduced on-station time and greater reliance on tanker aircraft. Although this limitation is not unique to the Block 2B or Block 3i configuration, the F-35 has high fuel burn rates and slow air refueling rates that extend air refueling times and decrease overall on-station time, which may reduce overall mission effectiveness.

- The program was able to improve stability of the mission systems software to support the Air Force's plan to declare IOC. The Program Office reported improvements in Mean Flight Hours Between Instability Events (MFHBIE) for both start-up and in-flight of Block 2B and Block 3i. The latest inflight stability metrics from the Program Office are provided in the table to the right. Note that "2BS" versions of software refer to Block 2B versions delivered to flight test. For Block 3i, the program adopted a naming convention where a "P" version refers to software released for production aircraft and an "R" version is for flight testing. An "R" version of software has additional coding that permits data to be collected from data buses on the aircraft and stored on the DART pod or transmitted to ground stations for recording or playback. For IOT&E, since data will be collected with the instrumentation packages on the OT aircraft, IOT&E will be flown with an "R" version of software where selected data and messages can be directed for recording for post-flight analyses.
- The operational effect of mission systems software instabilities on the F-35 will not be well understood before the completion of formal operational testing. One of the objectives of the Air Force IRA was to examine the frequency and effect of these instability events. The Air Force defined and scored instability events during the IRA in the same way as the Program Office and the contractor for comparison purposes and observed similar trends. An instability event is generally the initial failure, or the primary system failure, and does not account for subsequent failures of the same system or failures of subsystems. In addition, the Air Force collected data on instability occurrences, which includes a broader set of instabilities. An instability occurrence accounts for all failures of systems and associated subsystem failures, when each of the failures could have affected the mission capability of the aircraft. The Air Force collected data on instability occurrences with F-35A aircraft flying the most current Block 3i software and counted 25 occurrences in 34.1 flight hours, resulting in a Mean Flight Hours Between Instability Occurrences of 1.4 hours. During IOT&E, all relevant stability events and occurrences, on the ground or in the air, which impact mission effectiveness or suitability, including repeat events (unless attributed to a hardware failure) will be counted to assess overall mission effect. Similar to the table below, stability data from IOT&E will be compared with data from fielded aircraft with the "P" version of Block 3F software to assess any differences.

- The Air Force IRA test team at Nellis AFB flew a total of 18 mission scenarios (72 aircraft sorties) covering the mission sets of CAS, Air Interdiction (AI), and SEAD/DEAD. The missions were flown over the Western Test Ranges from March 1 through April 29, 2016. Additionally, the assessment included observations from an Air Force-led deployment to Mountain Home AFB, Idaho, with six F-35A

MISSION SYSTEMS SOFTWARE INFLIGHT STABILITY METRICS (DATA AS OF NOVEMBER 27, 2016)

Software Release	Number of Inflight Stability Events	Cumulative Flight Hours	Mean Flight Hours Between Instability Events
2BS5.2	31	224.8	7.3
2BS5.3	1	28.5	Insufficient data
3iP6.21	13	349.5	26.9
3iR6.21 (Edwards OT Aircraft)	6	75.8	12.6
3FR5*	222	950.1	4.3

* 3FR5 metrics are a summation of 8 versions of software used in flight testing: 3FR5, 3FR5.02, 3FR5.03, 3FR5.03QRC, 3FR5.04QRC, 3FR5.05, 3FR5.06, and 3FR5.07

aircraft from Edwards, supported by an ALIS SOU v2 with software 2.0.1. Although the Air Force has determined that the F-35A with Block 3i mission systems software provides "basic" capabilities for IOC, many significant limitations and deficiencies remain. In comparison to a dedicated operational test and evaluation, this was a brief, but revealing assessment of mission capability. However, until a full operational test and evaluation of the F-35 is completed, we will have low confidence that we understand all of the limitations in the system.

- The detailed results of the IRA, as reported by the Air Force, are consistent with the assessments in this Annual Report.
- Inflight stability of the Block 3i mission systems was assessed to be back to a level comparable to that in Block 2B, as measured by the number of inflight instability events per flight hour.
- If used in combat, F-35 aircraft will need support to locate and avoid modern threat ground radars, acquire targets, and engage formations of enemy fighter aircraft, due to unresolved performance deficiencies and limited weapons carriage available (i.e., two bombs and two air-to-air missiles).
- Unresolved Block 3i deficiencies in fusion, EW, and weapons employment continue to result in ambiguous threat displays, limited ability to effectively respond to threats, and, in some cases, a requirement for offboard sources to provide accurate coordinates for precision attack.
- Concerning the CAS mission area, the team concluded that the Block 3i F-35A does not yet demonstrate equivalent CAS capabilities to those of fourth generation aircraft.

Mission Data Load Development and Testing

- F-35 effectiveness in combat relies on mission data loads (MDL) – which are a compilation of the mission data files needed for operation of the sensors and other mission systems – working in conjunction with the system software data load to drive sensor search parameters so that the F-35 can identify and correlate sensor detections, such as threat and friendly radar signals. The contractor team produced an initial set of mission data files for developmental testing during SDD, but the operational MDLs – one for each potential major geographic area of operation – are being created, tested, and verified by a U.S. government lab, the U.S. Reprogramming Lab (USRL), located at Eglin AFB, Florida, which is operated by government personnel from the Services. The Air Force is the lead Service. These MDLs will be used for operational testing and fielded aircraft, including the Marine Corps and Air Force IOC aircraft. The testing of the USRL MDLs is an operational test activity, as was arranged by the Program Office after the restructure that occurred in 2010. The Department must have a reprogramming lab that is capable of rapidly creating, testing and optimizing MDLs, and verifying their functionality under stressing conditions representative of real-world scenarios, to ensure the proper functioning of F-35 mission systems and the aircraft's operational effectiveness in both combat and the IOT&E of the F-35 with Block 3F.
- Despite the critical requirement for developing and fielding F-35 MDLs, significant ongoing software and hardware deficiencies in the USRL have yet to be addressed, which continue to prevent efficient creating, testing, and optimization of the MDLs for operational aircraft fielded in the Block 2B and Block 3i configuration, and are preventing the development of MDLs for Block 3F.
  - The current reprogramming hardware and software tools are so cumbersome that it takes months for the USRL to create, test, optimize, and verify a new MDL. This time-consuming process was still not complete for the complete set of Block 3i AOR-specific MDLs.
  - The program has mismanaged sustainment and upgrades of the USRL to the point that it currently does not have the ability to start creating MDFs for Block 3F and will not have that capability until February 2017, at the earliest. Once the USRL can start creating Block 3F MDFs, it will take approximately 15 months to deliver a verified MDL for IOT&E and for fielded Block 3F aircraft.
  - The program plans to start delivering production aircraft in the Block 3F configuration in May 2017. Because the USRL will not be able to develop, test, and validate a Block 3F MDL until mid-2018, the Services will have to field Block 3F-capable aircraft with either Block 3i, or with a Block 3F test MDL provided by the contractor; however, either course of action will likely restrict these fielded Block 3F aircraft from use in combat.
- Additionally, the Program Office and Lockheed Martin have failed to complete necessary contracting actions to address current shortfalls in signal generation capability within the USRL, including the key hardware upgrades needed to create, test, and verify Block 3F MDFs to detect and identify emissions from currently fielded threat systems in scenarios with realistic threat densities. This failure occurred in spite of the requirement being clearly identified in 2012 and the Department programming $45 Million in the FY13-16 budgets to address it. The JPO sponsored a gap analysis study of USRL capabilities to determine the lab upgrade requirements at the engineering level before beginning contracting actions. When completed in 2014, the study concluded that between 16 and 20 upgraded radio frequency (RF) signal generator channels would be needed for the USRL to adequately create and test MDFs in the USRL for the fielded threats examined in the study, using realistic scenarios and threat densities. After receiving a proposal for the upgrades from the contractor priced at over $200 Million in May 2016, the JPO requested a new proposal, reportedly with options only for up to 12 upgraded signal generator channels, which the contractor indicated would not be answered until July 2017. Furthermore, once on contract, it would then take approximately 3 years after ordering the equipment for it to be delivered and installed, which will be late to need for

both IOT&E and fielding of Block 3F aircraft. As a result, even though the USRL will eventually have the capability to create MDLs for Block 3F in 2017, it still will not have the required signal generators to test and optimize the MDLs to ensure adequate performance against currently fielded threats.

- To provide the necessary and adequate Block 3F mission data development capabilities for the USRL, the Program Office must immediately fund and expedite the contracting actions for the necessary hardware and software modifications, including an adequate number of additional RF signal generator channels and the other required hardware and software tools. Unless these actions are taken immediately, the USRL will not be configured to create, test, and verify Block 3F MDLs for aircraft for current threat systems and threat scenarios until sometime in 2020, placing the operational aircraft at risk in combat against fielded threats and the program at risk of failing IOT&E. The program is working to find alternative facilities with the required signal generators to mitigate this lab capability shortfall for Block 3F.
- Significant additional investments are also required within 2-3 years to further upgrade the USRL to support F-35 Block 4 Follow-on Modernization (FoM) MDL development. Block 4.2 is currently planned to include new Technical Refresh 3 (TR3) processors and other new hardware which, due to the overlapping Block 4 increments, will require the USRL, or an additional reprogramming lab, to have two different avionics configurations simultaneously – a TR2 line for Blocks 3F and 4.1, plus a TR3 line for Block 4.2 and later. Although the Block 4 hardware upgrades in the USRL will need to begin soon to be ready in time, the reprogramming requirements for Block 4 have yet to be fully defined. The Program Office must expeditiously undertake the development of those requirements and plan for adequate time and resources within the DOD budget cycle, in order to ensure the USRL is able to meet Block 4 MDL requirements.
- The USRL, with JOTT observers, held an "Urgent Reprogramming Exercise (URE)" from April 20 to July 25, 2016. This type of exercise is intended to test the USRL's ability to respond to an urgent request from a Service to modify the mission data in response to a new threat or new mode of an existing threat. Due to USRL's ongoing production efforts, the URE was conducted concurrently with the lab's effort to produce an operational MDL, which is why the exercise period was several months, instead of a few days. The JOTT and USRL carefully tracked hours that were specific to the URE as they occurred and surveyed USRL personnel to identify process issues. The total hours recorded were double the Air Force standard for rapidly reprogramming a mature system. The JOTT identified several key process problems, many of which are described above, including the lack of necessary hardware, analysis tools that were not built for operational use, and missing capabilities, like the ability to quickly determine ambiguities in the mission data. These problems must be corrected in order to bring the USRL's ability to react to new threats up to the identified standards routinely achieved on legacy aircraft.
- In addition to the above deficiencies that involve overall laboratory capability and tools to develop MDLs, there are also deficiencies in the program's sustainment efforts to ensure a high state of readiness, particularly if the Services have an urgent reprogramming requirement at any time. To meet these tasks, the USRL must have all necessary equipment in a functioning status, similar to aircraft availability. Inadequacies in the current level of sustainment include, but are not limited to:
  - Insufficient number of Field Service Engineers (FSE) to assist in maintenance and operation of the lab equipment, which include both specialized equipment and aircraft mission equipment
  - Inadequate or insufficient training for most laboratory personnel, which is hindered by the insufficient number of FSEs
  - No engineering drawings or JTD for many critical components, making troubleshooting of failures of those components difficult and lengthening the time required to return the laboratory to full operational status
  - Insufficient spare parts for many critical components
  - Low supply priority, equivalent to that of a unit in training, resulting in long delays to receive required parts
  - Missing part numbers for many components, forcing USRL personnel to submit an Action Request (AR) first to determine the part number before a replacement part can be ordered through supply.

Weapons Integration and Demonstration Events

Block 3F Developmental Testing

- After the release of Block 3iP6.21 software in May 2016, the program focused on completing development of Block 3F capabilities, including weapons envelope and integration testing. To provide an operational employment flight envelope, the program accomplished flight sciences testing of external weapons carriage and employment, as well as integrating bombs (SDB-I, JSOW C-1, and PW-IV) and missiles (AIM-9X and AIM-132 ASRAAM) not previously integrated on the F-35 in Block 2B or 3i.
- The TEMP requires 26 Block 3F weapons delivery accuracy (WDA) events be completed as part of the Block 3F developmental testing effort. These WDAs are key developmental test activities necessary to ensure the full Block 3F fire-control capabilities support the "find, fix, track, target, engage, assess" kill chain. As of the end of November, only 5 of the 26 events (excluding the gun events) had been completed and fully analyzed. Several WDAs have revealed deficiencies and limitations to weapons employment. An additional 11 WDAs have occurred, but analyses are ongoing. Of the 10 remaining WDAs, 4 are still blocked due to open deficiencies that must be corrected before the WDA can be attempted. The program should correct deficiencies that are preventing completion of all of

the TEMP-required Block 3F WDA events and ensure they are completed prior to finishing SDD.

- Discoveries from the Block 3F WDA events include:
  - AIM-9X and AIM-132 ASRAAM seeker status tone problems
  - Out-of-date launch zones for AIM-120 missiles
  - Pilot Vehicle Interface (PVI) and mission planning problems with the U.S. Navy's JSOW-C1 missile that, if not corrected, may cause significant weapon employment limitations in the fleet's ability to attack moving ship targets and enable flexible engagement of land-based targets of opportunity
  - Ongoing radar and fusion deficiencies affecting air-to-air target track stability and accuracy, which could cause reduced missile lethality
  - Multiple hung stores, which typically result in an inflight emergency, occurred with the AIM-9X due to mission systems software and weapon integration deficiencies
  - Problems with integrating the British AIM-132 ASRAAM missile and Paveway IV bomb; changes to address these problems could have unintentionally affected the U.S. AIM-9X and laser-guided bomb capabilities, which may require regression testing of these U.S. weapons.
- In an effort to efficiently accomplish the WDA events, the program dedicated several test aircraft to a WDA surge period during June through August. Although the program had planned to begin WDA events as early as February 2016, the first live weapons event did not occur until July. Delays in starting the Block 3F WDAs were caused by immature software and deficiencies affecting weapons employment. The following table lists the Block 3F WDA events, software versions, scheduled and completion dates, overall results and assessments for each completed live fire event through the end of November. Many of the events were originally blocked from completion due to software deficiencies that had to be addressed using QRC versions of software in order to allow the weapons events to proceed.

Block 3F Developmental Testing Weapons Events Accomplished Through November 2016						
WDA Number	Weapon Event	Software Configuration	Scheduled Date	Completion Date	Result	Assessment
301	AMRAAM	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Initial data analysis indicates that there was an inflight issue that may have affected targeting accuracy. Analysis in process to determine the root cause and impact(s).
302	AMRAAM with AIM-9X	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Initial data review indicated that the AIM-9X tones were not as expected and there was no missile post-launch timer indication to the pilot.
303	AMRAAM fired with target off-boresight	3FR5.03	Feb 16	Aug 16	Partially successful accomplishment; shot captured key radar capability data but failed primary test objective; shot required control room intervention.	Known issues with outdated F-35 AMRAAM Attack Model in mission systems software resulted in no shoot cues or dynamic launch zone displayed to pilot requiring the control room to provide a "shoot" call to the pilot. Initial data review indicates that there was also no post-launch timer indication to the pilot. Also, weapon quality track was erratic pre- and post-launch. More detailed analyses are pending, following data to be provided by the missile vendor.
307	2 X AMRAAM	3FR5.03	Jun 16	Aug 16	Partially successful accomplishment; shot required control room intervention.	The cockpit indication was a guidance failure on the missiles and required control room intervention to confirm the shot parameters and direct the pilot to shoot. More detailed analyses are pending, following data to be provided by the missile vendor.
308	2 X SDB-I (GBU-39) and 1 X AMRAAM	3FR5.06	Jun 16	Nov 16	Successful accomplishment of event.	All weapons initially appear to have functioned successfully. Analysis ongoing.
311	2 X AMRAAM	3FR5.03	Apr 16	Jul 16	Pending Data Review; shot required control room intervention.	Unsuccessful; also the pilot indications in the cockpit indicted a guidance fail resulting in control room intervention to accomplish the shot. More detailed analyses are pending, following data to be provided by the missile vendor.
316	AIM-9X fired against a non-maneuvering target	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Inflight weapon failed on first missile attempt (built-in test failure and no missile tone to the pilot); back-up missile functioned as expected. Deficiency report was written on missile tone anomalies.
317	AIM-9X fired against a maneuvering target	3FR5.03	Jun 16	Aug 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Initial data review indicates that the missile tones were not correct, no dynamic launch zone indication in Dogfight mode and the gun symbology occluded the target in the helmet-mounted display. More detailed analyses on radar track accuracy and radar ranging accuracy following data to be provided by the missile vendor.
320	JDAM (GBU-31) delivered against a single target using Synthetic Aperture Radar (SAR) map coordinates	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team planned to use a known workaround for minor Launch Acceptability Region (LAR) inaccuracy due to an outdated LAR model in mission systems software. Pilot released the bomb using a "rule of thumb" guidance to determine "in-zone." JDAM LAR model update in mission systems software is required.
321	JDAM (GBU-31) delivered against a single target using Bomb-on-Coordinate employment	3FR5.03	Apr 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team planned to use a known workaround for a minor LAR inaccuracy due to an outdated LAR model in mission systems software. Pilot released the bomb using a "rule of thumb" guidance to determine "in-zone." Post-mission initial data review indicates that the target elevation values available to the pilot were not consistent between the mission planned terrain elevation, the displayed elevation on the cockpit displays, and the value loaded into the JDAM in the transfer alignment.

Block 3F Developmental Testing Weapons Events Accomplished Through November 2016 (CONTINUED)						
WDA Number	Weapon Event	Software Configuration	Scheduled Date	Completion Date	Result	Assessment
322	JDAM (GBU-31) X 2 Ripple release on two targets	3FR5.03	Jun 16	Aug 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team planned to use a known workaround for a minor LAR inaccuracy due to an outdated LAR model in mission systems software. Pilot released the bomb using a "rule of thumb" guidance to determine "in-zone." Pilot released weapons on rule-of-thumb with minor impact for this DT scenario and Service representatives have stated that the rule-of-thumb workaround may be adequate for operations. Post mission data analysis showed a SAR map coordinate inaccuracy, but within the Circular Error Probable (CEP) of the weapon.
323	JDAM (GBU-31) Pattern on target (multiple weapons)	3FR5.05	Jul 16	Oct 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Weapons impacted as expected with the selections made by the pilot and with accurate PVI indications. Dual voltage bomb rack unit (BRU) functioned properly with no power distribution issues.
324	SBD-I (GBU-39) X 2 on two targets	3FR5.03	May 16	Aug 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team used a planned workaround for BRU-61; using the new dual-voltage BRU in single-voltage mode due to a mission systems software limitation.
325	SDB-I (GBU-39) Single release	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team used a U.S. non-operationally representative BRU-61, one with only a single voltage unit, to complete this WDA event. This older BRU-61 is representative for partner operations.
328	UK Paveway IV bomb	3FR5.05	Jul 16	Oct 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	Weapons integration deficiencies were identified during this event and deficiency reports completed.
SDB Seps	SDB-I (GBU-39) multiple ripple release for flight sciences separation test points, completed on mission systems aircraft.	3FR5.03	Feb 16	Jul 16	Successful accomplishment of event and sufficient data collected for weapons integration analyses.	The test team used a U.S. non-operationally representative BRU-61, one with only a single voltage unit, to complete this WDA event. This older BRU-61 is representative for partner operations. Awaiting data delivery for detailed analysis.

- The remaining 10 events are planned to be completed over the next several months, as the program provides versions of Block 3F software with necessary deficiency fixes to allow the rest of the events to proceed. The remaining events are complex multi-weapon, multi-target, and advanced threat presentations. Whether all WDAs will be completed with the final planned increment of Block 3F software – version 3FR6 – released in December is still to be determined, but several key deficiency fixes related to weapons employment are apparently not included and the probability of additional discoveries during the remaining weapons test events is high, based on results to date.

Gun Testing

- All three variants add gun capability with Block 3F. The F-35A gun is internal; the F-35B and F-35C each use a gun pod. Differences in the outer mold-line faring mounting make the gun pods unique to a specific variant, i.e., a gun pod designated for an F-35B cannot be mounted on an F-35C aircraft.
- Flight sciences testing of the F-35A internal gun was completed in May 2016. The first firing of the gun in flight occurred October 30, 2015, and the entire flight sciences test effort consisted of 11 flights over the 7-month period. Testing revealed that the small doors that open when the gun is fired induce a yaw (i.e., sideslip), resulting in gun aiming errors that exceed accuracy specifications. As a result, software changes to the flight control laws were needed to enable adjustments, which are still to be determined by flight testing, to cancel out the yaw when the gun doors are open. These control law changes, and the resulting regression testing, delayed the start of gun accuracy flight testing on mission systems test aircraft until December 2016, at the earliest. Since no mission-systems-capable developmental test aircraft were built with an internal gun, the program modified one of the operational test F-35A aircraft (AF-31) to conduct the needed gun testing events. Until testing is completed on AF-31, it is unknown if the F-35 gun system, aimed by the Gen III HMDS, will meet accuracy requirements for effective air-to-air and air-to-ground gun employment.

- The program has conducted ground testing of the F-35B gun pod and plans to start airborne testing in January 2017. Initial ground firing of the F-35C gun pod occurred in mid-November 2016 and airborne gun testing is planned to start in March 2017. New discoveries, as well as determining the amount of adjustment to the flight control laws to counter the pitching moments induced by firing the gun pod, are likely.
- Accuracy testing of the gun with the HMDS has not yet been completed and continues to be delayed as new discoveries are made. Hence, the effectiveness of the gun, aimed via the gunsight in the HMDS, is still unproven for both air-to-air and air-to-ground gun employment. The effects of the canopy transparency on gun aiming – i.e., the pilot aiming the gun via the HMDS gunsight looking through the thick canopy material, associated distortions, and attempted software-programmed corrections – are not yet characterized.
- Although aimed firing of the gun had yet to occur, both DT and OT pilots have flown with the air-to-ground gun strafing symbology displayed in the helmet and reported concerns that it is currently operationally unusable and potentially unsafe to complete the planned aimed gun fire testing. These deficiencies may cause further delays to the start of gun accuracy flight testing. Also, testing of the air-to-air symbology by both DT and OT pilots revealed that the gunsight is very unstable when tracking a target aircraft. Fixing these deficiencies may require changes to the mission systems software that controls symbology to the helmet, or to the radar software, as the program is working to finalize the last version of Block 3F. Plans to begin aimed flight testing of the gun on the F-35A were planned for this fall, but will likely not start until December 2016, at the earliest.
- Because of the late testing of the gun and likelihood of additional discoveries, the program's ability to deliver gun capability with Block 3F before IOT&E is at risk, especially for the F-35B and F-35C, which have not yet fired the gun in flight.

Weapons Demonstration Events by the Operational Test Teams

- The JOTT and the associated Service operational test squadrons (VMX-1, 31TES, and 422TES) assigned to Edwards AFB, California, and Nellis AFB, Nevada accomplished 6 air-to-air missile events, 19 GBU-31/32 JDAM air-to-ground events, and 28 GBU-12 laser guided bomb events during 2016. For one of these events, the team accomplished one combined AMRAAM missile with one GBU-12 laser guided bomb event, as described in the AMRAAM Air-to-Air Missile Event Table on the following page. These weapon delivery events were accomplished on range complexes at the Naval Weapons Center China Lake, California; Marine Corps Air Station Yuma, Arizona; and Eglin AFB, Florida. All of the OT weapon events were planned and accomplished in operationally representative scenario profiles constructed to evaluate the F-35's ability to find-fix-track-target-engage-assess airborne and fixed and moving ground targets.
- The following tables and accompanying assessments show the weapon events, aircraft Block configuration, date accomplished, and results.

AMRAAM Air-to-Air Missile Events Accomplished by Operational Test Teams				
Event Identifier	**Event Description**	**Aircraft Block Software Configuration**	**Date Accomplished**	**Results**
WDA-108	Cruise Missile Defense	3iR6.01	May 16	This event was a re-shoot of a developmental test event. The reshoot was required by the operational test community because of control room workarounds needed during the DT event. The OT profile was successful.
OT 2.1	2 F-35 aircraft in MADL network attacking one F-16 drone target with jamming	2BR5.3	Aug 16	Profile did not meet test objectives due to issues with the target presentation. Data analysis in progress.
OT 2.2	2 F-35 aircraft in MADL network defending against an off-boresight attacker	2BR5.3	Aug 16	Partially successful. Missile guided to objective target, however secondary objective compromised due to issues with the target presentation. Data analysis in progress.
OT 2.3	2 F-35 aircraft in MADL network vs 2 jamming equipped F-16 drones	2BR5.3	Aug 16	Profile did not meet test objectives due to issues with the target presentation. Data analysis in progress.
OT 2.4	F-35 combined Air-to-Air AMRAAM and GBU-12 Air-to-Ground profile	2BR5.3	Aug 16	Primary test objective to confirm ability of the F-35 to support a laser guided bomb to impact while simultaneously supporting a missile inflight was successful. Secondary objective was unsuccessful due to issues with the target presentation.
MAWTS-2	2 F-35 aircraft attacking a high closure rate supersonic target	2BR5.3	Aug 16	This profile was a USMC engagement scenario to support ongoing tactics development. Profile objective was successful

Air-to-Air General Observations

- The operational test teams completed the missile profiles in accordance with the DOT&E-approved test plan; however, some weapons integration objectives were not successful due to the drone target presentation failures (details are classified). The failures in the drone target presentations prevented either the primary or secondary test objectives to verify the F-35's capability to complete the find-fix-track-target-engage-assess fire control thread. The test team is conducting data analyses to determine whether engineering characterization runs or re-shooting of the profiles are required.
- Although four of the five missile events fell short of addressing all of the specific data objectives, they were successful in identifying key deficiencies in the ability of the aircraft to support selected missile functionality, stores management system anomalies, and the instability of the shoot cues provided to the pilot to support missile employment. Data analyses to identify root cause for all the noted deficiencies are ongoing and the operational test team will recommend specific mission systems software fixes to address the noted deficiencies.

GBU-31/32 Joint Direct Attack Munition (JDAM) and GBU-12 Laser Guided Bomb (LGB) Air-to-Ground Event Summary				
Weapon Type	**Number of Weapons Events**	**F-35 Variant******	**Date Accomplished**	**Results**
GBU-12 LGB	28 Laser Guided Bomb (LGB) Events*	21 F-35A	Jan to July 2016	22 successful/6 partially successful*** events.
		7 F-35B		
GBU-31 or GBU-32 JDAM	15 GBU-31 (BLU-109) Events (8 inert/7 live)**	F-35A		10 successful/5 partially successful***
	3 inert GBU-32 (Mk-83) Events**	F-35B		2 successful/1 partially successful***

*GBU-12 OT events were conducted against an operationally representative mix of fixed and moving targets; self-, airborne buddy-, and ground tactical control party target-lasing; target cueing via voice, VMF digital, and F-35 shoot-list sharing via MADL.
**JDAM GBU-31/32 events were accomplished against an operationally representative mix of fixed target coordinates consisting of: pre-planned targeted coordinates, F-35 self-targeting using SAR map and EOTS derived coordinates, and target cueing via voice, VMF digital, and F-35 shoot-list sharing via MADL.
***Air-to-Ground fully successful missions achieved weapon miss distances within expected mean radial error. Partially successful missions were cases where the weapon was employed but with larger miss distances and observed mission systems issues described below.
****Mission Systems software for all variants was 2BS5.2 or 2BS5.3

Air-to-Ground General Observations

- Although initial observations from weapons integration can be characterized in general, detailed data analyses are ongoing to determine precise mean radial error results for both the LGB and JDAM weapons delivery events, and to identify root causes for the observed mission systems deficiencies and weapon delivery issues.
- The JDAM predictive launch acceptability region (LAR) and dynamic launch zone (DLZ) information were consistently in error compared to the expected pilot drop cues calculated from both the JDAM truth model and initial DT characterizations. In the majority of the OT JDAM drops, there were wide discrepancies between the LAR presentations to the pilot via the HMDS, the corresponding presentations on the in-cockpit controls and displays, and the actual JDAM in-weapon LAR. In a number of cases, the mission systems bombing cues available to the pilot via the Tactical Situation Display on the Panoramic Cockpit Display were in conflict with the HMDS shoot cues and the DLZ. This inconsistency is both confusing to the pilot and can result in erratic and inaccurate weapon impact relative to the target desired impact point. Also, the tactical displays available to the pilot did not allow the pilot to confirm the actual target coordinates passed to the weapon. This confirmation of the in-weapon target coordinates is usually required by rules of engagement (ROE) in operational areas in order to enable positive target information confirmation to the ground controllers prior to clearance to drop any weapon. The F-35 in the Block 2B or Block 3i configuration is not currently able to comply with these ROE.
- In general, pilots were able to use the F-35 Synthetic Aperture Radar (SAR) mapping function to derive weapons quality coordinates, which are adequate to deliver ordinance on target. Pilots were also able to share the SAR-map-derived coordinates between flight members to validate and confirm target positions and coordinates prior to releasing weapons.
- The EOTS was not able to provide the pilot with sufficient resolution at tactical employment ranges to enable a positive ID on the intended target. However, the EOTS generally was able to track targets, both moving and stationary, but only after the target identification was confirmed by an external source or multiple sources. However, there are still significant tracking limitations, as evidenced by a new, open Category 1-High deficiency titled "EOTS TFLIR Tracker Unable to Point or Area Track." The EOTS system also was able to generate accurate weapon quality coordinates when cued to the correct target.
- The lack of any lead-point-compute or lead-laser guidance in the F-35 EOTS system required rule-of-thumb pilot techniques to provide limited capability with the GBU-12 on moving targets. The OT moving target attacks were generally successful; however, the successes relied on high levels of pilot experience and were not enabled by the F-35 mission systems. While the rule-of-thumb procedures allowed the technical requirements of the weapons delivery event to be met, they did not allow the pilot to maintain positive target ID using the PVI procedures to designate, track, and employ the weapon for the full attack timeline. Most importantly, these procedures would likely not have met the current positive target ID requirements for operational employment rules of engagement. Due to these limitations, which threaten the effectiveness of the F-35 to engage moving targets, the program and Services are exploring other options to meet this ORD requirement. One option, which is being considered by the Air Force, is to integrate the GBU-49, a fielded weapon that has similar size, weight, and interfaces as the GBU-12, or a similar weapon that does not require lead-laser guidance, in Block 3F. Otherwise, the program plans to develop and field lead-laser guidance in Block 4.2, which would be delivered in CY22, at the earliest. However, because of the similarities, the GBU-49 could be quickly integrated with Block 3F to provide a robust moving target capability for the F-35 much earlier.
- Pilots were able to use the digital Variable Message Format (VMF) system to communicate between F-35 aircraft and tactical ground controllers. The VMF links and data provided the expected data to both the pilot and the ground parties. In previous developmental testing, the VMF has exhibited significant issues with both reliability and accuracy; however, in the OT events the system was both reliable and accurate. Data analysis is ongoing to determine the differences between the uses of VMF in developmental testing compared to the operational weapons test events. The ground parties used in the operational testing were equipped with the most up-to-date software, firmware, and hardware and were staffed by fully qualified ground controllers.
- Pilots experienced multiple inflight failures of the Fuselage Remote Interface Unit (FRIU), an electronic component that provides the interface between the aircraft avionics and all weapon stations, which often disrupted the ground attack profile. The failures resulted in degraded weapons at critical phases of the target attack profile and required the pilots to abort the attack, reset the FRIU to regain control and communications with the weapon, and then recommit to a follow-on target attack. Such target attack interruptions are unacceptable for combat operations.
- Pilots consistently rated the Offboard Mission Support (OMS) mission planning system as cumbersome, unusable, and inadequate for operational use. As a result, the time required for operational planners to build a mission plan is excessive and cannot support current planning cycle requirements for multiple aircraft combat missions. Additionally, the post-mission download times are too long to support operational debriefing requirements.

Pilot Escape System

- Testing of the pilot escape system in CY15 showed that the risk of serious injury or death is greater for lighter-weight pilots, which led to the decision by the Services to restrict pilots weighing less than 136 pounds from flying the F-35.

In an effort to reduce this risk, the program developed three modifications associated with the escape system and began testing them in late CY15 and throughout CY16. These modifications include:
- Reduction in the weight of the pilot's Generation III helmet (the new helmet is called Gen III Lite) to reduce the effect of forces on the pilot's neck during the ejection sequence.
- Installation of a switch in the seat that allows lighter-weight pilots to select a slightly delayed activation of the main parachute. This delay allows the drogue chute, which deploys almost immediately during the ejection sequence, to further slow and align the pilot before the main parachute deploys. This delay is designed to reduce the severity of loads on the neck experienced during opening shock.
- The addition of a Head Support Panel (HSP) between the risers of the parachute designed to prevent the pilot's neck from "snapping back" through the risers during the opening of the main parachute.

- Concerned with the problems with the escape system and the possibility of more discoveries, the U.S. Air Force asked the JPO in June 2016 to gather and provide information on potential costs and challenges to changing ejection seats from the Martin Baker US16E seat currently installed in all F-35 variants to the United Technologies ACES 5 seat as an alternative for the F-35A.
- After prototypes of the design changes were available, twenty-two qualification test cases were completed between October 2015 and September 2016, with variations in manikin weight, speed, altitude, helmet size and configuration, and the seat switch settings. Seven of the tests were accomplished with the lightweight (103 lbs) manikin. Data from these tests showed that the HSP significantly reduced neck loads under conditions that forced the head backwards, inducing a rearward neck rotation, during the ejection sequence. Data also showed that the seat switch delay reduced the opening shock from the main parachute for lighter-weight pilots at speeds greater than 160 knots. Results of the additional tests were provided to the Services in late CY16 to update their risk assessments associated with ejections. Despite the improved results, the extent to which risks have been reduced to lighter-weight pilots (i.e., less than 136 pounds) by the modifications to the escape system and helmet is still to be determined by these analyses. If the Services accept the risk associated with the modifications to the escape system for pilots weighing less than 136 pounds, restrictions will likely remain in effect until aircraft have the modified seat with the switch and HSP installed, and the Gen III Lite helmets are procured and delivered to the applicable pilots in the fleet.
- The program plans to start retrofitting fielded F-35s with the modifications to the ejection seats in February 2017 and delivering aircraft with the upgraded seat in Lot 10, starting in January 2018. The Gen III Lite helmets will be included with the Lot 10 aircraft delivery, and will be delivered starting in November 2017. If these delivery timelines are met, the Air Force may open F-35 pilot training to lighter-weight pilots (i.e., below 136 pounds) as early as December 2017.
- Part of the weight reduction to the Gen III Lite HMDS involved removing one of the two visors (one dark, one clear). As a result, pilots that will need to use both visors during a mission (e.g., during transitions from daytime to nighttime), will have to store the second visor in the cockpit. However, there currently is not adequate storage space in the cockpit for the visor; the program is working a solution to address this problem.
- The program has yet to complete additional testing and analysis needed to determine the risk of pilots being harmed by the Transparency Removal System (which shatters the canopy first, allowing the seat and pilot to leave the aircraft) during ejections in other than ideal, stable conditions (such as after battle damage or during out-of-control situations). Although the program completed an off-nominal rocket sled test with the Transparency Removal System in CY12, several aspects of the escape system have changed since then, including significant changes to the helmet, which warrant additional testing and analyses. DOT&E recommends the program complete these tests, in a variety of off-nominal conditions, as soon as possible, so that the Services can better assess risk associated with ejections under these conditions.

Static Structural and Durability Testing

- Structural durability testing of all variants using full-scale test articles continues, with plans for each variant to complete three full lifetimes (one lifetime is 8,000 equivalent flight hours, or EFH). Although all variants are scheduled to complete testing before the end of SDD, the complete teardown, analyses, and damage assessment and damage tolerance reporting is not scheduled to be completed until August 2019. Testing on all variants has led to discoveries requiring repairs and modification to production designs and retrofits to fielded aircraft.
- F-35A durability test article (AJ-1) completed the second lifetime of testing, or 16,000 EFH in October 2015. After completing second lifetime inspections, third lifetime testing began on March 11, 2016. As of November 16, 2016, 20,000 EFH, or 50 percent of the third lifetime had been completed. Third lifetime testing is projected to complete in December 2017.
- F-35B durability test article (BH-1) completed 14,051 EFH by November 17, 2016, which is 6,051 hours (76 percent) into the second lifetime. Due to the amount of modifications and repairs to bulkheads and other structures in the current F-35B ground test article, it may not be adequate to continue testing and a new one may be needed and durability testing repeated to ensure adequate lifetime testing is completed. The program needs to conduct an assessment to determine the extent to which the results of further durability testing are representative of production aircraft and if necessary procure another test article for the third life testing.

- Two main wing carry-through bulkheads, FS496 and FS472, are no longer considered production-representative due to the extensive repairs that have been required. The program plans to continue durability testing, repairing the bulkheads as necessary, through the second lifetime (i.e., 8,001 through 16,000 EFH), which is projected to be complete in February 2017.
- Prior to CY16, testing was halted on September 29, 2013, at 9,056 EFH, when the FS496 bulkhead severed, transferred loads to, and caused cracking in the adjacent three bulkheads (FS518, FS472, and FS450). The repairs and an adequacy review of the repairs to support further testing were completed on December 17, 2014, when the program determined that the test article could continue testing. Testing restarted on January 19, 2015, after a 16-month delay.
- The program determined that several of the cracks discovered from the September 2013 pause at 9,056 EFH were initiated at etch pits. These etch pits are created by the etching process required prior to anodizing the surface of the structural components; anodizing is required for corrosion protection. Since the cracks were not expected, the program determined that the etch pits were more detrimental to fatigue life than the original material design suggested. The program is currently developing an analysis path forward to determine the effect on the overall fatigue life.
- After the durability test completed 11,915 EFH on August 13, 2015, the load cycling was stopped to allow removal and replacement of the FS496 bulkhead outer segments (both left- and right-hand sides), removal and replacement of the left-hand-side aft fuselage close-out frame, repairs to the engine thrust mount shear webs, installation of fasteners at the FS518 frame, maintenance of the right-hand-side EHAS panel, repairs to the right-hand-side of the mid-fairing longeron, and repairs to the FS556 upper arch. The entire repair activity took about 9 months, with an 85-EFH testing effort conducted in early March 2016 that reached 12,000 EFH.
- Testing resumed in early May 2016, reached 13,000 EFH in mid-June 2016, and then stopped for another month to repair the FS472 lower flange.
- Testing resumed in mid-July. At 13,086 EFH, cracks were discovered on the forward fuselage including FS236 bulkhead, left-hand-side FS223 frame, and right-hand-side FS191 upper frame.
- Testing continued with buffet loads until it reached 13,980 EFH before stopped to implement fuselage repairs in August 2016.
- Testing resumed on September 17 and had reached 14,051 EFH on November 17, 2016.

• F-35C durability test article (CJ-1) completed the second lifetime of testing, or 16,000 EFH on October 29, 2016. The third lifetime testing is scheduled to begin in late December 2016.

- In October 2015 with 13,731 EFH accomplished, cracks were discovered on the left-hand side and right-hand side of one wing front spar and one left-hand-side wing forward root rib; this discovery was considered significant because wing spar and wing root rib are primary structural components and the cracks were not predicted by the finite element model (FEM) used in the design of these components. The repairs took over 3 months before the test resumed in early February 2016.
- On February 9, 2016, with 13,827 EFH accomplished, a crack was found on the left-hand-side inverter/converter/controller and power distribution center/inverter bay floor. Testing continued with catapult and trap load cycling.
- In late February 2016 with 13,931 EFH accomplished, cracks were found on the left- and right-hand sides of the FS496 bulkhead flanges, which were deemed significant. The repairs took another 3 months to complete before the test resumed in May 2016.
- In August 2016 with 14,831 EFH accomplished, small cracks were found on the right-hand-side armpit (below wing root) and were quickly repaired with a simple blend.
- In August 2016 with 14,892 EFH accomplished, cracks were found on the FS518 lower frame and some nearby broken fasteners. A weld repair for the titanium frame was completed. Further investigation revealed cracks on the right- and left-hand-side wing rear spars. While a repair disposition was being developed, the durability test resumed with loading only for catapult takeoffs and carrier trap landings.

• The program plans to use Laser Shock Peening (LSP), a mechanical process designed to add compressive residual stresses in the materials, in an attempt to extend the lifetime of the FS496 and FS472 bulkheads in the F-35B. The first production line cut-in of LSP will start with Lot 11 F-35B aircraft. Earlier Lot F-35B aircraft will undergo LSP processing as part of a depot modification. Testing is proceeding in three phases: first, coupon-level testing to optimize LSP parameters; second, element-level testing to validate LSP parameters and quantify life improvement; and third, testing of production and retrofit representative articles to verify the service life improvements. All three phases are in progress, with full qualification testing scheduled to be completed in August 2017. As of December 1, 2016, 122 of 211 durability tests had been conducted with results within expectations, which is a 58 percent completion.

Joint Simulation Environment (JSE)

• The JSE is a man-in-the-loop, mission systems software-in-the-loop simulation developed to meet the operational test requirements for Block 3F IOT&E. The Program Office made the decision in September 2015 to stop development on the contractor's effort to build a similar system, the Verification Simulation (VSim), instead tasking the Naval Air Systems Command (NAVAIR) to lead the building of a government-owned Joint Simulation Environment (JSE), with the contractor providing only the F-35 aircraft and sensor models. However, negotiations for the F-35 models have not yet been successful, which has prevented NAVAIR from fully defining the simulation's architecture and environment (the virtual software environment in which aircraft, sensor, and threat models interact with one another).

- While the Program Office continued to negotiate with the contractor, and had success in meeting the hardware requirements (facilities, cockpits, etc.), the lack of definition of the simulation environment makes any integration schedule not credible. In the next year, the program must acquire the F-35 models, integrate them into an as-yet undefined and undeveloped battlespace environment, complete development of several dozen threat aircraft and surface system models, ensure that aircraft sensor models correctly perceive the threat system models, and validate the entire simulation. Previous efforts of this magnitude have taken several years, so it is unlikely that NAVAIR will complete the project as planned in time to support IOT&E. Current Program Office estimates are that JSE will deliver late to need in May 2019, but before the end of IOT&E. Verification, Validation, and Accreditation (VV&A) activities remained effectively stalled in 2016 and are also a very high risk to timely completion of the simulation.
- Without a high-fidelity simulation, the F-35 IOT&E will not be able to test the F-35's full capabilities against the full range of required threats and scenarios. Nonetheless, because aircraft continue to be produced in substantial quantities (essentially all of which require modifications and retrofits before being used in combat), the IOT&E must be conducted without waiting for the JSE, to demonstrate F-35 combat effectiveness under the most realistic conditions that can be obtained in flight testing, once the aircraft hardware and software meet the IOT&E entrance criteria, which is expected to occur long before the completion and successful VV&A of JSE. It is now clear that the JSE will not be available and accredited in time to support the Block 3F IOT&E. The currently approved IOT&E detailed test design, which was developed entirely around open-air flight testing, mitigates the lack of an adequate simulation environment as much as possible.

Live Fire Test and Evaluation (LFT&E)

F-35C Full-Scale Aft Fuselage and Empennage Structure Test

- The F-35 LFT&E program completed the F-35C full-scale aft fuselage and empennage structure tests. The Navy's Weapons Survivability Laboratory in China Lake, California, accomplished three test events using the CG:0001 full scale structural test article. The tests evaluated the ability of the vertical tail and aft boom structure to withstand damage from high-explosive incendiary (HEI) projectile and simulated Man-Portable Air Defense System (MANPADS) threats. A preliminary review of the test results indicates that:
  - The F-35 vertical tail is capable of withstanding an HEI projectile impact. The threat can target and fail one attachment lug but the remaining lugs demonstrated their ability to handle normal flight loads after the impact. However, the pilot receives no alerts from the Integrated Caution, Advisory and Warning (ICAW) system from this type of structural damage, so there is a potential that a damaged vertical tail could fail without warning the pilot if the pilot demands higher than normal flight loads on the vertical tail after the damage occurs.
  - Two MANPADS shots were completed against the aft boom structures, which support the horizontal and vertical tails. Combined with results from earlier tests on an F-35A and F-35B test articles, these tests showed that the structures are sufficiently robust against these threats to retain all control surfaces. Although damage to a single control surface actuator is possible, earlier flight control tests showed sufficient controllability within a limited flight envelope to allow controlled flight back to a safe area where the pilot could eject.
  - The MANPADS tests demonstrated the potential for damage to the fueldraulics system – the engine fuel-based hydraulics system – which can result in a sustained fire leading to further damage to the aircraft and a pilot ejection over enemy territory. The data will be used to support an assessment in 2017 that will determine the contribution of this issue to the overall aircraft vulnerability.
  - While extended fires occurred in the MANPADS tests, there has been no effort expended to determine what catastrophic damage might result and the timeframe for that to occur. Current procedures are for an immediate ejection upon determination of a sustained fire. However, if the time-to-failure could be established for this sort of fire, it might allow the pilot time to depart a combat area and eject somewhere relatively safe. Further analysis of these test results and the related issue are needed.

PAO Shut-Off Valve

- The program has not provided an official decision to reinstate this vulnerability reduction feature. There has been no activity on the development of the PAO-shut-off valve technical solution to meet criteria developed from 2011 live fire test results. As stated in several previous reports, this aggregate, 2-pound vulnerability reduction feature, if installed, would reduce the probability of pilot incapacitation, decrease overall F-35 vulnerability, and prevent the program from failing one of its vulnerability requirements.

Vulnerability to Unconventional Threats

- The full-up, system-level chemical-biological decontamination test on an SDD aircraft, which began 4QFY16 and is scheduled to end in 2QFY17 at Edwards AFB, was supported by two risk-reduction events:
  - A System Integration Demonstration of the proposed decontamination equipment and shelter was conducted on an F-16 test article during 1QFY15 at Edwards AFB to simulate both hot air chemical and hot/humid air biological decontamination operations. Extensive condensation inside the shelter and on the test article during the

hot/humid air biological decontamination event indicated the need for process and shelter modifications.
  - A 2QFY16 event demonstrated that a modified system process and a better insulated shelter can maintain adequate temperature and humidity control inside the shelter, even in a cold-weather environment.
- The test plan to assess chemical and biological decontamination of pilot protective equipment is not adequate. Compatibility testing of protective ensembles and masks has shown that the materials survive exposure to chemical agents and decontamination materials and processes, but the program has neither tested nor provided plans for testing the HMDS currently being fielded. Gen II HMDS compatibilities were determined by analysis, comparing HMDS materials with those in an extensive DOD aerospace materials database. A similar analysis is planned for the Gen III HMDS design. However, even if material compatibilities were understood, there are no plans to demonstrate a process that could adequately decontaminate either HMDS from chemical and biological agents.
- The Joint Program Executive Office for Chemical and Biological Defense approved initial production of the F-35 variant of the Joint Service Aircrew Mask (JSAM-JSF) during 1QFY16. This office and the F-35 Joint Program Office are integrating the JSAM-JSF with the HMDS, which is undergoing Safety of Flight testing.
- The Navy evaluated an F-35B aircraft to the EMP threat level defined in Military-Standard-2169B. Follow-on tests on other variants of the aircraft, including a test series to evaluate any Block 3F hardware/software changes, are planned for FY16-17.

Gun Ammunition Lethality and Vulnerability

- The 780th Test Squadron at Eglin AFB, Florida, completed the ground-based lethality test of the PGU-47/U Armor Piercing High Explosive Incendiary with Tracer (APHEI-T) round (also known as Armor Piercing with Explosive (APEX)) against armored and technical vehicles, aircraft, and personnel-in-the-open targets. Ground-based lethality tests for the APEX correlated well with pre-test predictions for the round penetrations, but potential problems were discovered with fuze functioning when impacting rolled homogeneous armor at high obliquity. Nammo, the Norwegian manufacturer, conducted additional testing to identify the cause of the dudded rounds during the ground tests and subsequently modified the fuze design to increase reliability. The program will determine the effect of the ground-based lethality test data on the ammunition lethality assessment.
- Per the current mission systems software schedule, the weapons integration characterization of the gun and sight systems will not be ready for the air-to-ground gun strafe lethality tests until December 2016, at the earliest. Strafing targets will include a small boat, light armored vehicle, technical vehicle (pickup truck), and plywood mannequins for each round type tested.

Operational Suitability

- The operational suitability of all variants continues to be less than desired by the Services. Operational and training units must rely on contractor support and workarounds that would be challenging to employ during combat operations. In the past year some metrics of suitability performance have shown improvement, while others have been flat or declined. Most metrics still remain below interim goals to achieve acceptable suitability by the time the fleet accrues 200,000 flight hours, the benchmark set by the program and defined in the Operational Requirements Document (ORD) for the aircraft to meet reliability and maintainability requirements. This level of maturity is further stipulated as 75,000 flight hours for the F-35A, 75,000 flight hours for the F-35B, and 50,000 flight hours for the F-35C.
- Reliability growth has stagnated, so it is highly unlikely that the program will achieve the ORD threshold requirements at maturity for the majority of reliability metrics, most notably the Mean Flight Hours Between Critical Failures, without redesigning aircraft components.
- Aircraft fleet-wide availability averaged 52 percent for 12 months ending October 2016, compared to the modest goal of 60 percent. It is important to note that the expected combat sortie rates will require significantly greater availability than 60 percent; therefore, if the F-35 is to replace legacy aircraft for combat taskings, availability will likely need to improve to near 80 percent.
- Monthly availability had been averaging in the mid-30s to low-40s percent for the 2-year period ending September 2014. Monthly availability then increased rapidly and significantly from October to December, peaking at 56 percent in December 2014. However, since then it has remained flat, centering around the low-50s percent with no strong improving trend over time.
- Only two out of nine reliability metrics that have ORD requirement thresholds have improved since last year's report. All nine are below the interim goals that were set to determine if the metrics will meet the thresholds by maturity. None are within 5 percent of their interim goal, whereas previously, several of these metrics were reported as being above or within 5 percent of their interim goal. In particular, reliability metrics related to critical failures have decreased over the past year. This decrease in reliability correlates with the simultaneously observed decline in the Fully Mission Capable (FMC) rate for all variants, which measures the percentage of aircraft not in depot status that are able to fly all defined F-35 missions. The fleet-wide FMC rate peaked in December 2014 at 62 percent and has fallen steadily since then to 21 percent in October 2016.
- In addition to the nine ORD metrics, there are three contract specification metrics, Mean Flight Hours Between Failure scored as "design controllable," or DC, one for each variant. DC failures are equipment failures due to design flaws considered to be the fault of the contractor, such as components not withstanding stresses expected to be found

in the normal operational environment. It does not include failures caused by improper maintenance, or caused by circumstances unique to flight test. This metric exhibited the highest rate of the growth in the past and, for this metric, all variants are currently above program target values for this stage in development. However, since May 2015, DC reliability has generally decreased or remained flat as well.

- Although most measures of reliability have not improved significantly over the past year, three of six measures of maintainability have improved slightly. Maintainability metrics record the amount of time required to troubleshoot and repair faults on the aircraft. Additionally, the number of flight hours each aircraft flies per month, known as the utilization rate, has also increased marginally.
- F-35 aircraft spent 9 percent more time down for maintenance than intended (fleet average of 16.4 percent compared to 15 percent goal), and waited for parts from supply for 71 percent longer than the program targeted (fleet average of 17 percent compared to goal of 10 percent). At any given time, from 10 to 20 percent of aircraft were in a depot facility or depot status at the home base for major rework or planned upgrades. Of the remaining aircraft not in any depot status, on average less than a third were able to fly all missions of even a limited capability set that is associated with the Block 2B or Block 3i aircraft.
- Accurate suitability measures rely on adjudicated data from fielded operating units. A Joint Reliability and Maintainability Evaluation Team (JRMET), composed of representatives from the Program Office, the JOTT, the contractor (Lockheed Martin), and Pratt and Whitney (for engine records), reviews maintenance data to ensure consistency and accuracy for reporting measures; government representatives chair the team. However, the Lockheed Martin database that stores the maintenance data, known as the Failure Reporting and Corrective Action System (FRACAS), was not in compliance with U.S. Cyber Command information assurance policies implemented in August 2015 through late summer of 2016. Because of this non-compliance, government personnel were not able to access the database via government networks, preventing the JRMET from holding regularly scheduled reviews of maintenance records for nearly a year, other than a few ad hoc reviews. Regular JRMET meetings resumed in September 2016, but the program is currently working through reviewing a large backlog of un-adjudicated field data. The program restarted publishing monthly reliability and maintainability (R&M) status reports from adjudicated data in October 2016, after roughly a year-long hiatus.

F-35 Fleet Availability

- Aircraft availability is determined by measuring the percent of time individual aircraft are in an available status, aggregated over a reporting period (e.g., monthly). The program assigns aircraft that are not available to one of three categories of status: Not Mission Capable for Maintenance (NMC-M); Not Mission Capable for Supply (NMC-S); and depot status.
  - Program goals for these not-available categories have remained unchanged since 2014, at 15 percent for NMC-M, 10 percent for NMC-S, and 15 percent of the fleet in depot status. Depot status is primarily for completing the modifications required to bring currently fielded aircraft in compliance with their expected airframe structural lifespans of 8,000 flight hours and to incorporate additional mission capability. The majority of aircraft in depot status are located at dedicated depot facilities for scheduled modification periods that can last several months, and they are not assigned as a part of the operational or training fleet during this time. A small portion of depot activity can occur in the field when depot field teams conduct a modification at a main operating base, or affect repairs beyond the capability of the local maintenance unit. Similar to being at a depot facility, aircraft are temporarily assigned to depot status during these periods and are not considered a part of the operational or training fleet.
  - These three not-available category goals sum to 40 percent, resulting in a fleet-wide availability goal of 60 percent for 2016.
  - In addition to these overall program goals, the program has implemented a Performance Based Logistics (PBL) construct with Lockheed Martin that ties contract incentive awards to a slightly different set of tailored fleet performance targets. These tailored targets prioritize improvement efforts for Marine Corps F-35B performance as the first branch to declare Initial Operational Capability (IOC), and also because the F-35B variant has shown the lowest overall availability performance. Current PBL-based goals are 53 percent availability, 35 percent FMC, and 70 percent mission effectiveness rates for the F-35B training and operational fleets assigned to Marine Corps Air Station (MCAS) Beaufort and MCAS Yuma. The majority of the incentive structure is tied to these goals. To ensure Lockheed Martin continues to try to improve performance across the board, a smaller portion of the incentive fee is tied to overall fleet performance metrics of 60 percent F-35A, 50 percent F-35B, and 60 percent F-35C availability, regardless of operating site.
- Aircraft monthly availability averaged 52 percent for the 12-month period ending October 2016 in the training and operational fleets, with a maximum availability of 55 percent in May 2016 and a minimum availability of 44 percent in October 2016. This is only a minor improvement over the average 51 percent monthly availability reported in the FY15 DOT&E Annual Report for the 12 months ending October 2015. Further, some groups of aircraft continue to experience minimum availability well below 50 percent.
  - In no month did the overall fleet exceed its goal of 60 percent availability. Only the F-35C variant exceeded the 60 percent goal, in 6 of 12 months, with a maximum availability of 71 percent in April 2016. The F-35A and F-35B variants never exceeded 60 percent, but the F-35A

achieved 59 percent in May 2016 and the F-35B reached a maximum 50 percent in January, April, and July 2016.

- The table below summarizes aircraft availability by operating location for the 12-month period ending October 2016. The first column indicates the average availability achieved for the whole period, while the maximum and minimum columns represent the range of monthly availabilities reported over the period. The number of aircraft assigned at the end of the reporting period is shown as an indicator of potential variance in availability. Sites are arranged in order of when each site began operation of any variant of the F-35, and then arranged by variant for sites operating more than one variant. The Marine Corps terminated F-35B operations at Eglin AFB in February 2015, so there were no F-35Bs at that site for the 12-month period of this report; thus, that entry, previously reported in the FY15 DOT&E Annual Report, has been removed. The Navy operational test squadron at Edwards AFB received its first F-35C in August 2016, the only new operating site to stand up since the FY15 DOT&E Annual Report.
- Trend analysis of monthly fleet availability from August 2012 through October 2016 showed a weak rate of improvement of approximately 5 percent growth per year over this period. This is consistent with the growth rate reported in the DOT&E FY15 Annual Report – but, again, the growth was neither steady nor continuous. The majority of this growth still results from a concentrated increase in availability that occurred during the months of September 2014 through December 2014. Analysis of availability from January 2015 through October 2016, the time period after this concentrated increase, shows a more modest less than 1 percent annual growth rate, which is in better agreement with recent observations.
- The combined fleet of designated, instrumented OT aircraft currently at Edwards AFB, which was built in Lots 3 to 5, averaged 48 percent availability from January to October 2016. Seventeen instrumented OT aircraft were assigned to Edwards AFB as of October 2016. This is well-short of the target of 80 percent that will be needed to conduct an efficient IOT&E, or combat operations.

F-35 AVAILABILITY FOR 12-MONTH PERIOD ENDING OCTOBER 2016[1]

Operational Site	Average	Maximum	Minimum	Aircraft Assigned[2]
Whole Fleet	52%	55%	44%	178
Eglin F-35A	38%	49%	32%	25
Eglin F-35C	60%	71%	54%	21
Yuma F-35B	55%	62%	40%	19
Edwards F-35A	53%	74%	40%	8
Edwards F-35B	46%	64%	30%	7
Edwards F-35C[3]	27%	40%	4%	2
Nellis F-35A	50%	62%	42%	13
Luke F-35A	61%	68%	44%	44
Beaufort F-35B	43%	53%	33%	24
Hill F-35A	57%	80%	22%	15

1. Data do not include SDD aircraft.
2. Aircraft assigned at the end of October 2016.
3. Edwards AFB F-35C operations began August 2016.

- Due to concurrent development and production, which resulted in delivering operational aircraft before the program has completed development and finalized the aircraft design, the Services must send the current fleet of F-35 aircraft to depot facilities. This is to receive modifications that have been designed since the aircraft were originally manufactured and are now required for full capability. Some of these modifications are driven by faults in the original design that were not discovered until after production had started, such as major structural components that do not meet the requirements for the intended lifespan, and others are driven by the continuing improvement of the design of combat capabilities that were known to be lacking when the aircraft were first built. These modifications are a result of the concurrency of production and development and cause the program to expend resources to send aircraft for major re-work, often multiple times, to keep up with the aircraft design as it progresses. Since SDD will continue at least to the middle of 2018, and by then the program will have delivered nearly 200 aircraft to the Services in other than the 3F configuration, the depot modification program and its associated concurrency burden will be with the Services for years to come.
  - Sending aircraft to depot facilities for several months at a time to bring them up to Block 3i capability from Block 2B (i.e., upgrading avionics processors) and to meet life limit requirements, and eventually to the Block 3F configuration, reduces the number of aircraft at field sites and thus decreases fleet availability. For the 12-month period ending October 2016, the proportion of the fleet in depot status averaged 15 percent, compared to 16 percent for the 12-month period ending October 2015 stated in the DOT&E FY15 Annual Report. The proportion of aircraft in depot status was relatively flat over the majority of this period with little overall trend, ranging between a maximum monthly value of 22 percent and a minimum value of 11 percent. The maximum value of 22 percent occurred in October 2016, and was partly driven by one-time repairs to shedding foam insulation around PAO lines in the fuel tanks for 15 fielded F-35A aircraft. DOT&E expects this rise in the depot rate to be a one-time occurrence, and not indicative of a general trend.
  - There is evidence from Program Office reports, however, that later production lot aircraft achieve higher availability rates than earlier lots. For example, for the period from October 2015 to September 2016, accounting for 30 Lot 4 aircraft of all variants, each variant averaged a monthly availability between 43 and 44 percent. For the same time period and accounting for 33 Lot 7 aircraft of all variants, each variant averaged a monthly availability between 64 and 68 percent, which was a statistically significant

increase. However, a significant amount of this increase in availability can be attributed to the newer lot aircraft requiring fewer depot modifications. Over this period the Lot 4 aircraft averaged a monthly depot rate between 19 and 26 percent, depending on variant, whereas the Lot 7 aircraft averaged a monthly depot rate between 0 and 6 percent, considering variant.

- Projections of depot rates beyond 2016 are difficult, since testing and development are ongoing and discoveries continue, including the need for redesigned outer wing structure on the F-35C to accommodate AIM-9X missile carriage. This structural modification was installed on an F-35C developmental test aircraft for testing in late 2016. Also, the program does not yet know the full suite of modifications that will be necessary to bring currently produced aircraft up to the final Block 3F configuration. However, as the program continues to ramp up production rates, the later lot aircraft, which generally require fewer modifications, will comprise a larger proportion of the fleet and may exert a downward influence on the depot percentage rate.

• To examine the suitability performance of fielded aircraft, regardless of how many are in the depot, the program reports on the Mission Capable (MC) and Fully Mission Capable (FMC) rates for the F-35 fleet. The MC rate represents the proportion of the fleet that is not in depot status and that is ready to fly any type of mission (as opposed to all mission types). This rate includes aircraft that are only capable of flying training flights, however, and not necessarily a combat mission. The FMC rate calculates only the proportion of aircraft not in depot status that are capable of flying all assigned missions and can give a better view into the potential combat capability available in the fielded units.

- F-35 aircraft averaged a 62 percent MC rate for the 12-month window ending in October 2016 considering all variants, a slight decrease from the 65 percent reported in the FY15 DOT&E Annual Report. The rate showed little change over time, ranging from a minimum value of 57 percent to a maximum value of 66 percent for the whole fleet, and was relatively consistent across variants as well. The F-35A achieved the highest variant-specific rate at 64 percent, followed by 63 percent for the F-35C, and 59 percent for the F-35B.
- The FMC rate continued to exhibit a steady decline first observed in 2015, and averaged only 29 percent over the period, compared to 46 percent reported in the FY15 DOT&E Annual Report. The rate started at 32 percent in November 2015, which was close to the peak of 33 percent in April 2016, but generally dropped month over month to a minimum value of 21 percent by October 2016. The FMC rate has not been consistent across variants. The F-35A fleet achieved the highest average FMC rate for the period at 37 percent, followed by the F-35C at 24 percent. The F-35B fleet exhibited only a 14 percent average FMC rate, however. Failures in the Distributed Aperture System (DAS), electronic warfare (EW) system, and Electro-Optical Targeting System (EOTS) were the highest drivers pushing aircraft into Partial Mission Capable (PMC) status.
- Analysis of the MC rate of each production lot reveals that later lot aircraft have a greater MC rate than earlier lot aircraft; the difference is less pronounced than the comparison of availability, but still significant. The 30 Lot 4 aircraft averaged between 52 and 61 percent MC over this period by variant, compared to 68 to 73 percent for the Lot 7 aircraft by variant.
- The OT fleet at Edwards AFB averaged an MC rate of 53 percent from January to October 2016.

• The first table below shows F-35 MC and FMC rates for the total fleet and each variant for the 12-month period ending October 2016, including the average, maximum, and minimum monthly values observed. The second table shows F-35 availability and MC rates by production lot and by variant for the 12-month period ending September 2016.

F-35 MC AND FMC RATES BY VARIANT FOR 12-MONTH PERIOD ENDING OCTOBER 2016

Variant	MC			FMC		
	Avg.	Max	Min	Avg.	Max	Min
Fleet	62%	66%	57%	29%	33%	21%
F-35A	64%	70%	55%	37%	42%	27%
F-35B	59%	65%	53%	14%	17%	10%
F-35C	63%	73%	55%	24%	44%	13%

F-35 AVAILABILITY AND MISSION CAPABLE RATES BY LOT (OCTOBER 2015 TO SEPTEMBER 2016)

Lot	No. of Aircraft				Availability			Mission Capable		
	F-35A	F-35B	F-35C	Total	F-35A	F-35B	F-35C	F-35A	F-35B	F-35C
2/3	14	13	-	27	33%	37%	N/A	57%	54%	N/A
4	10	17	3	30	44%	44%	43%	61%	59%	52%
5	22	3	7	32	51%	50%	57%	62%	52%	60%
6	23	6	7	36	62%	60%	67%	63%	66%	68%
7	22	7	4	33	67%	64%	68%	73%	68%	68%
8	14	3	3	20	49%	65%	79%	68%	65%	80%

- The monthly NMC-M rate averaged 16 percent over the period and was relatively stable, with a minimum value of 14 percent and a maximum value of 20 percent. This rate achieved the program goal of 15 percent, or lower, in 4 of the 12 months of the period. It also shows a slight decreasing (improving) trend over time that indicates with further improvement it may be possible to achieve and sustain program targets within the next calendar year.
  - Completing directed modifications or upgrades on still-possessed aircraft in the field also affects the NMC-M rate. In such cases, squadron-level maintainers, instead of the depot or contractor field teams, are tasked to complete Time Compliance Technical Directives (TCTDs). The "time compliance" limits for these directives vary, normally allowing the aircraft to be operated for a certain period of time without the modification. This permits maintenance personnel to do the work at an opportune time, without taking the aircraft off the flight schedule to do so, such as by combining the TCTD with other maintenance activities. While maintainers accomplish these TCTDs, the aircraft are designated as NMC-M status, and not in depot status. Incorporating these TCTDs will drive the NMC-M rate up (worse) until these remaining modifications are completed. Publishing and fielding new TCTDs is expected for a program under development and is needed to see improvement in reliability and maintainability; however, they inherently add to the maintenance burden in the fielded operational units.
- The NMC-S rate averaged 17 percent and showed no significant trend over the period. In no month did the rate achieve the program goal of 10 percent or less, with a minimum value of 14 percent and a maximum value of 20 percent.
  - Several factors have contributed to the NMC-S rate underperforming relative to its goal more than either the NMC-M or depot not-available categories. First, the program originally funded spares to a 20 percent NMC-S rate. To determine the quantity and type of spares needed to achieve this, the program used incorrect engineering predictions that overestimated component reliability (fleet data were not available when this modeling was done early in the program). Actual mean time between failures for many components is lower than the forecasted values used in the spares model. Second, contracting for spares has often been late to need to support the first aircraft delivery for several of the initial production lots. Third, the program has been late to stand up organic depot capabilities to repair existing parts that have failed but can be refurbished instead of being replaced with new parts. Such a capability would reduce the strain on suppliers to produce more spare parts.
  - The lack of spares available in the supply system is driving operating units to take good parts from one NMC aircraft and install them in other aircraft down for those parts, bringing the latter back to available status. This process, known as cannibalization, is performed by units when supply cannot provide needed parts in a timely manner. Cannibalization results in a significant increase in maintenance man-hours compared to replacing a bad part with a new or repaired part. For the 12-month period ending in October 2016, the monthly cannibalization rate averaged 9.8 cannibalization actions for every 100 sorties against a program goal of no more than 8 actions for every 100 sorties. The fleet met this goal in only 1 month, performing 6.2 cannibalizations per 100 sorties in December 2015, but analysis over this period does not demonstrate a statistically significant trend in the cannibalization rate.
  - Modifying aircraft also has an effect on the NMC-S rate as the Services can cannibalize parts from aircraft in the depots to support field units when replacement parts are not otherwise available from normal supply channels or stocks of spare parts on base. With the large number of aircraft in depot status, the program may have been able to improve the NMC-S rate by using depot cannibalizations, instead of procuring more spare parts, or reducing the failure rate of parts installed in aircraft, or improving how quickly failed parts are repaired and returned to circulation. If the Services endeavor to bring all of the early lot aircraft into the Block 3F configuration, the program will continue to have an extensive modification program for several years. While this will continue to provide opportunities for depot cannibalizations during that time, once the Block 3F modifications are complete, there will be fewer aircraft in the depot serving as spare parts sources and more in the field requiring parts support. If demand for spare parts remains high, this will put pressure on the supply system to keep up with demand without depot cannibalization as a source.
  - While the fleet was much closer to achieving the NMC-M goal than the NMC-S goal, these two rates are not necessarily completely independent. Specifically, poor diagnostics or difficult-to-conduct troubleshooting – issues that are maintainability problems at root cause – can drive the NMC-S rate up as well. For example, if troubleshooting efforts initially isolate faults to incorrect parts, units may inadvertently take good parts off the aircraft, return them to the supply system for depot or manufacturer checks, and demand replacement parts, unnecessarily straining the supply system for repair actions that will not resolve the fault. Units will report aircraft in NMC-S status until these replacement parts arrive. Once the unit receives and installs these parts, it would discover that the original problem remains, and return the aircraft to NMC-M status until further troubleshooting hopefully isolates the correct part. Thus, actions to reduce higher-than-targeted NMC-S rates may include improving the accuracy of diagnostics and troubleshooting procedures as well as increasing the availability of spare parts.
- The following table summarizes depot, NMC-M, and NMC-S rates for the total F-35 fleet and each variant for the 12-month period ending October 2016, including the average, maximum, and minimum monthly values observed.

F-35 DEPOT, NMC-M, AND NMC-S RATES BY VARIANT FOR 12-MONTH PERIOD ENDING OCTOBER 2016									
Variant	Depot (Goal of 15% or less)			NMC-M (Goal of 15% or less)			NMC-S (Goal of 10% or less)		
	Avg.	Max	Min	Avg.	Max	Min	Avg.	Max	Min
Fleet	15%	22%	11%	16%	20%	14%	17%	20%	14%
F-35A	14%	27%	8%	17%	24%	12%	17%	21%	12%
F-35B	20%	25%	14%	17%	25%	11%	16%	20%	13%
F-35C	6%	15%	2%	14%	20%	9%	20%	27%	13%

- Low availability is preventing the fleet of fielded operational F-35 aircraft from achieving the originally planned, Service-funded flying hour goals. The original Service beddown plans were based on F-35 squadrons ramping up to a steady state, fixed number of flight hours per tail per month, allowing for the projection of total fleet flight hours.
  - Since poor availability in the field has shown that these original plans were unexecutable, the Program Office has since produced modeled-achievable projections of total fleet flight hours, basing these projections on demonstrated fleet reliability and maintainability data, as well as expectations for future improvements. The most current modeled-achievable projection is from March 2016.
  - Through November 21, 2016, the fleet had flown approximately 91 percent of the modeled-achievable hours. This is an improvement since November 2015, the date used in the FY15 DOT&E Annual Report, when the fleet had flown 82 percent of modeled-achievable hours; however, recent updates to the model revised the projected hours downward. The completion of actual flight hours against modeled-achievable flight hours was consistent across all three variants, with each variant completing between 90 or 96 percent of its variant-specific projection. By comparison, the fleet had flown only 72 percent of the original beddown plan hours, with wide discrepancy between variants. The F-35A had flown 82 percent of its original beddown plan hours, while the F-35C had flown only 49 percent, for example.
  - The following table shows the planned versus achieved flight hours by variant for both the original plans and the modeled-achievable projections for the fielded production aircraft through November 21, 2016.

F-35 FLEET PLANNED VS. ACHIEVED FLIGHT HOURS AS OF NOVEMBER 21, 2016						
Variant	Original Beddown Plan Cumulative Flight Hours			"Modeled Achievable" Cumulative Flight Hours		
	Est. Planned	Achieved	Percent Planned	Est. Modeled	Achieved	Percent Planned
F-35A	41,000	33,754	82%	36,788	33,754	92%
F-35B	29,000	19,644	68%	21,935	19,644	90%
F-35C	12,500	6,070	49%	6,348	6,070	96%
Total	82,500	59,469	72%	65,071	59,469	91%

F-35 Fleet Reliability

- Aircraft reliability assessments include a variety of metrics, each characterizing a unique aspect of overall weapon system reliability.
  - Mean Flight Hours Between Critical Failures (MFHBCF) includes all failures that render the aircraft not safe to fly, and any equipment failures that would prevent the completion of a defined F-35 mission. It includes failures discovered in the air and on the ground.
  - Mean Flight Hours Between Removal (MFHBR) gives an indication of the degree of necessary logistical support and is frequently used in determining associated costs. It includes any removal of an item from the aircraft for replacement. Not all removals are failures, and some failures can be fixed on the aircraft without a removal. For example, some removed items are later determined to have not failed when tested at the repair site. Other components can be removed due to excessive signs of wear before a failure, such as worn tires.
  - Mean Flight Hours Between Maintenance Event Unscheduled (MFHBME_Unsch) is a useful reliability metric for evaluating maintenance workload due to unplanned maintenance. Maintenance events are either scheduled (e.g., inspections, planned removals for part life) or unscheduled (e.g., maintenance to remedy failures, troubleshooting false alarms from fault reporting or defects reported but within limits, unplanned servicing, removals for worn parts— such as tires). One can also calculate the mean flight hours between scheduled maintenance events, or total events including both scheduled and unscheduled. However, for this report, all MFHBME_Unsch metrics refer to the mean flight hours between unscheduled maintenance events only, as it is an indicator of aircraft reliability and the only metric with an ORD requirement for mean flight hours between maintenance event.
  - Mean Flight Hours Between Failures, Design Controllable (MFHBF_DC) includes failures of components due to design flaws under the purview of the contractor, such as the inability to withstand loads encountered in normal operation. Failures induced by improper maintenance practices are not included.
- The F-35 program developed reliability growth projection curves for each variant throughout the development period as a function of accumulated flight hours. These projections were established to compare observed reliability with target numbers to meet the threshold requirement at maturity, defined by 75,000 flight hours for the F-35A and F-35B, and by 50,000 flight hours for the F-35C, for a total 200,000 cumulative fleet flight hours. In November 2013, the program discontinued reporting against these curves for all ORD reliability metrics, and retained only the curve for MFHBF_DC, which is the only reliability metric included in the JSF Contract Specification (JCS). DOT&E reconstructed the growth curves for the other metrics analytically for this report. The following discussion and tables compare the

3-month reliability metrics to the growth goals required to be on track to meet threshold requirements at maturity.

- As of the end of July 2016, the F-35 fleet, including operational and flight test aircraft, had accumulated nearly 60,300 flight hours, or approximately 30 percent of the total 200,000-hour maturity mark defined in the ORD. Unlike the above table, which accounts only for fielded production aircraft, the flight test aircraft are included in the fleet hours which count toward reliability growth and maturity. By variant, the F-35A had flown approximately 32,400 hours, or just over 43 percent of its individual 75,000-hour maturity mark; the F-35B had flown approximately 20,300 hours, or 27 percent of its maturity mark; and the F-35C had flown approximately 7,600 hours, or 15 percent of its maturity mark.

- The program reports reliability and maintainability metrics on a 3-month rolling window basis. This means, for example, the MFHBR rate published for a month accounts only for the removals and flight hours of that month and the two previous months. This rolling 3-month window provides enough time to average out variability often seen in month-to-month reports, while providing a short enough period to distinguish current trends.
- The first table, below, compares the most recently reported and projected interim goal MFHBCF values, with associated flight hours. It shows the ORD threshold requirement at maturity and the values for May 2015, the month used in the FY15 DOT&E Annual Report, for reference as well.
- The three similar tables on the next page compare the most recently reported and projected interim goals for MFHBR, MFHBME_Unsch, and MFHBF_DC rates for all three variants. MFHBF_DC is contract specification, and its JCS requirement is shown in lieu of an ORD threshold.
- Note that data more current than July 2016 were not available at the time of this report due to the backlog of maintenance events awaiting JRMET review as a result of the Lockheed Martin database (FRACAS) not being compliant with all applicable DOD information assurance policies mandated by U.S. Cyber Command.
- Reliability values decreased (worsened) for 8 of 12 metrics between the May 2015 and the July 2016 values. All three MFHBCF metrics decreased between May 2015 and July 2016, and usually showed the greatest degree of reduction compared to the other reliability metrics. This aligns with the declining FMC rates for all variants. Of the remaining metrics, F-35A MFHBR and MFHBME_Unsch, and F-35A and F-35B MFHBF_DC, improved slightly. A more in-depth trend analysis over the 12-month period showed that all three variants exhibited declining MFHBCF; F-35B and F-35C MFHBR and MFHBME_Unsch were either flat or decreasing slowly; and MFHBF_DC for all variants were also either flat or decreasing. Only F-35A MFHBR and MFHBME_Unsch increased over this period.
- All nine of the ORD metrics are below interim program goals based on their planned reliability growth curves to meet threshold values by maturity. Furthermore, none of the ORD metrics are within 5 percent of their interim goals. Of the ORD metrics, F-35B MFHBME, at 86 percent, was the closest to its interim goal, while F-35C MFHBCF, at 39 percent, was the farthest. All of the JCS metrics, which are the MFHBF_DC for each variant, are above their growth curve interim values, ranging from 12 percent above for the F-35A to 28 percent above for the F-35B. This pattern indicates that the performance of the contract specification reliability metrics exceeding their interim values is not translating into the ORD reliability metrics showing the same improvement, which are operational requirements that will be evaluated during IOT&E.
- The fact that all the contract specification metrics are above their growth curve does not necessarily imply that the F-35 will deliver desired reliability in the field, especially in light of the fact that all ORD requirements are below their growth curves. The ORD requirements reflect how the aircraft will perform in combat, while the JCS metrics are limited to failures that are definitively the fault of component design. However, several situations can divorce improvement in the JCS metrics to similar improvements in the ORD metrics or availability. For example, components that are easily broken during maintenance, such as nutplates, may not be scored as design-controllable failures, but repairing and replacing these fragile components will adversely affect the ORD reliability metrics. Likewise, when old versions of redesigned components fail in the field, depending on circumstances, these failures may not be reported in the reliability metrics, but the effect on downing the aircraft will always be reflected in the availability metrics.
- The effect of lower (poorer) MFHBCF values is reduced aircraft fully mission capable, mission capable, and

F-35 RELIABILITY: MFHBCF (HOURS)								
Variant	ORD Threshold		Values as of July 31, 2016				Values as of May 2015*	
	Flight Hours	MFHBCF	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBCF	Observed MFHBCF (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Cumulative Flight Hours	Observed MFHBCF (3 Mos. Rolling Window)
F-35A	75,000	20	32,358	17.8	8.0	45%	15,845	8.8
F-35B	75,000	12	20,256	10.0	4.6	46%	11,089	7.2
F-35C	50,000	14	7,648	10.9	4.2	39%	3,835	7.5

* The JPO revised past R&M metrics based on applying the current JRMET scoring rules to past data. As a result, values reported for May 2015 in this report may be different than the values for the same month in the FY15 DOT&E Annual Report. See the Reliability Growth section below for more details.

F-35 RELIABILITY: MFHBR (HOURS)								
Variant	ORD Threshold		Values as of July 31, 2016				Values as of May 2015	
	Flight Hours	MFHBR	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBR	Observed MFHBR (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Cumulative Flight Hours	Observed MFHBR (3 Mos. Rolling Window)
F-35A	75,000	6.5	32,358	5.8	4.7	81%	15,845	4.4
F-35B	75,000	6.0	20,256	5.0	2.8	56%	11,089	4.0
F-35C	50,000	6.0	7,648	4.7	2.3	49%	3,835	3.9

F-35 RELIABILITY: MFHBME_Unsch (HOURS)								
Variant	ORD Threshold		Values as of July 31, 2016				Values as of May 2015	
	Flight Hours	MFHBME_ Unsch	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBME_Unsch	Observed MFHBME_Unsch (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Cumulative Flight Hours	Observed MFHBME_Unsch (3 Mos. Rolling Window)
F-35A	75,000	2.0	32,358	1.77	1.36	77%	15,845	1.13
F-35B	75,000	1.5	20,256	1.25	1.08	86%	11,089	1.10
F-35C	50,000	1.5	7,648	1.13	0.74	65%	3,835	0.98

F-35 RELIABILITY: MFHBF_DC (HOURS)								
Variant	JCS Requirement		Values as of July 31, 2016				Values as of May 2015	
	Flight Hours	MFHBF_ DC	Cumulative Flight Hours	Interim Goal to Meet JCS Requirement MFHBF_DC	Observed MFHBF_DC (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Cumulative Flight Hours	Observed MFHBF_DC (3 Mos. Rolling Window)
F-35A	75,000	6.0	32,358	5.2	5.8	112%	15,845	5.4
F-35B	75,000	4.0	20,256	3.2	4.1	128%	11,089	3.6
F-35C	50,000	4.0	7,648	2.9	3.3	114%	3,835	4.2

availability rates. MFHBR values lagging behind planned growth targets drive a higher demand for spare parts from the supply system than originally envisioned. When MFHBME_Unsch values are below expectation, there is a higher demand for maintenance manpower than anticipated.

Reliability Growth

- In the fall of 2016, the Program Office revised reliability and maintainability (R&M) metrics that had been previously reported by applying new or updated JRMET scoring rules that had been created or modified at different times over the course of system development, and agreed to by the JRMET members, to historical maintenance event data. Scoring rules determine such criteria as when a maintenance event is considered relevant and should be included in R&M metrics, when an event is not relevant and will not be included in metrics, such as failures in test-specific instrumentation that will not be installed in operational aircraft, and when an event is chargeable to the design-controllable metric as being the fault of the design as opposed to induced by improper maintenance. There are many detailed scoring rules to ensure similar maintenance situations are scored consistently. As the JRMET developed new scoring rules and changed some existing ones, the program realized that previously reported metrics needed to be revised – scored by the new rule set – in order to ensure current R&M metrics could be compared more accurately with past R&M performance. The effects on each reliability metric of this revision were mixed, with 7 of 12 of the May 2015 metrics being revised downward (worsening), and the remaining 5 increasing compared to their originally reported values; however, 4 of these improved metrics decreased, or worsened, by July 2016. Note the values in the tables above reflect the JPO revised past R&M metrics based on applying the current JRMET scoring rules to past data. As a result, values reported for May 2015 in this report may be different than the values for the same month in the FY15 DOT&E Annual Report.
- In the two prior Annual Reports, DOT&E reported the results of reliability growth analysis based on the Duane Postulate, using R&M data provided by the Program Office, to determine the rate of growth for MFHBR and MFHBME_Unsch. In 2016, DOT&E conducted an updated analysis of reliability growth using the more refined U.S. Army Materiel Systems Analysis Activity (AMSAA)-Crow model, examining data from the start of the program to July 2016. The AMSAA-Crow model characterizes growth by a single growth parameter, using a method that is similar to the Duane Postulate. A growth rate between zero and one implies improvement in reliability, a growth rate of zero

implies no growth, and a growth rate less than zero implies reliability decay. Since it is logarithimic, a growth rate of 0.40 represents much faster than twice the growth of a rate of 0.20.

- Unlike the Duane Postulate, the AMSAA-Crow model enables the determination of statistical confidence intervals on its estimated growth rate based on the underlying mathematics in the model. Further, the expected growth rate is determined by Maximum Likelihood Estimator (MLE) methods, rather than linear regression as in the Duane Postulate, allowing for the quantity of data to have an effect on the growth parameter estimate.
  - Previous DOT&E Annual Report reliability growth analyses included only the F-35A and F-35B variants, and only for the MFHBR and MFHBME metrics, due to a small amount of hours on the F-35C, and fewer critical failures than removals and unscheduled maintenance events. For this year's updated analysis, sufficient data for the MFHBCF metric and the F-35C variant were available for these metrics and estimates to be included.
  - The first table below shows the most likely growth rate and 95 percent upper and lower confidence bound growth rates, providing a range of likely values for the actual growth rate, for all three variants and all three ORD reliability metrics. It also includes the projected values of these three metrics for each variant based on the most likely, upper, and lower bound growth rates at maturity; i.e., 75,000 flight hours for the F-35A and F-35B and 50,000 flight hours for the F-35C.

Metric	Variant	July 2016 Growth Rates			Projections at Maturity			ORD Threshold
		Most Likely	Lower Bound	Upper Bound	Most Likely	Lower Bound	Upper Bound	
MFHBCF	F-35A	0.137	0.109	0.164	9.6	9.0	10.2	20.0
	F-35B	-0.051	-0.089	-0.014	N/A *			12.0
	F-35C	-0.107	-0.180	-0.039	N/A *			14.0
MFHBR	F-35A	0.192	0.173	0.211	6.1	5.8	6.4	6.5
	F-35B	0.126	0.103	0.148	4.1	3.9	4.4	6.0
	F-35C	-0.068	-0.119	-0.020	N/A *			6.0
MFHBME _Unsch	F-35A	0.170	0.161	0.179	1.38	1.35	1.41	2.0
	F-35B	0.359	0.351	0.367	2.01	1.96	2.08	1.5
	F-35C	0.189	0.174	0.205	1.26	1.20	1.33	1.5

* No estimates for projections at maturity were made for metrics with negative growth rates.

Aircraft	MFHBME_Unsch Growth Rate
F-15	0.14
F-16	0.14
F-22 (at 35,000 flight hours)	0.22
B-1	0.13
"Early" B-2 (at 5,000 flight hours)	0.24
"Late" B-2	0.13
C-17 (at 15,000 flight hours)	0.35

  - The growth rates listed in the first table were calculated with approximately 32,400 hours for the F-35A, 20,300 hours for the F-35B, and 7,600 hours for the F-35C. For comparison, historically observed MFHBME_Unsch growth rates for several currently fielded aircraft are shown in the second table. Analogous rates for MFHBR and MFHBCF are not available.
- The updated reliability growth analysis through July 2016, using the AMSAA-Crow model, accounts for the recent tapering off of reliability growth better than the Duane Postulate. As a result, most of the growth rates in the table above are lower than those reported in prior DOT&E Annual Reports. For the nine ORD metrics, the current growth analysis predicts that only one will meet or surpass the ORD threshold value at maturity, F-35B MFHBME_Unsch. As the analysis showed no growth for F-35B and F-35C MFHBCF, and F-35C MFHBR, no projections out to maturity were made for those metrics and current estimates do not meet threshold requirements.
  - Comparing the currently exhibited MFHBME_Unsch growth rates to historical aircraft shows that from program initiation to July 2016, F-35 reliability has improved faster than average for all variants. However, F-35 reliability remains below program interim goals for its current stage of development in all cases, and is not projected to achieve threshold values by maturity in most cases, due to very low initial reliability at the start of the program, well below the assumed initial reliability values that informed program interim goals.
  - Although there were approximately 7,600 hours on the F-35C fleet for this year's analysis, usually enough time to establish a growth trend, the lack of evidential growth in the MFHBCF and MFHBR metrics may be explained by the fact that the F-35C fleet has only recently begun to send aircraft to the depot for modifications. Also, the F-35C fleet has the least hardware improvements incorporated relative to the F-35A and F-35B fleets. The relatively strong growth in the MFHBME metric, by contrast, can be partly explained for all variants by a reduction in false alarms from the aircraft Prognostics and Health Management (PHM) system, driving fewer overall unscheduled maintenance actions, in addition to the natural learning curve process.
- Based on current reliability trends, projections to maturity may not be appropriate. Reliability growth projection methodologies often assume that a system is in a single phase of testing, characterized by a nearly constant operating mode and environment, and gets reliability improvements incorporated while the system is under test. For most of the F-35 program, these conditions have held sufficiently true such that reliability growth displayed consistent behavior; however, with the release of Block 2B capabilities, including increased flight envelope, beginning in 2015, both the operating mode and environment apparently changed enough to constitute a new phase for the purpose of analyzing reliability growth. Programs with multiple phases

of development, where each phase is defined by different environments or operational usage, normally generate separate reliability planning curves (used to determine interim goals during that phase) and separate reliability growth tracking curves for each phase, as a single curve is not sufficient to mathematically represent reliability growth behavior across multiple phases. Because the reliability projections are based on data that span the periods of time, both before and after the Block 2B fleet release, they may not best capture reliability trends.

- For programs with multiple phases, it is common for reliability to decrease or level off at the start of a new phase when the system is subjected to a more stressing operating mode or environment that exposes new failure modes. As a result, reliability growth can come to a halt or even decline; however, after a while, growth may resume as the program starts to implement reliability improvements for these new failure modes.
- Reliability growth may resume as a result of ongoing program reliability improvement initiatives, continuing to send aircraft through the depot modifications program, replacing lower reliability components with higher reliability versions via TCTDs, and other reliability initiatives. However, DOT&E also expects that the Block 3F envelope and capabilities release, incrementally released between CY17 and CY18, will reveal new failure modes (e.g., new weapons, higher airspeeds and g with Block 3F envelope) that will limit the overall effect of these reliability improvement initiatives.
- Despite the difficulty projecting accurate reliability values at maturity, given the phased introduction of F-35 block capabilities, DOT&E does not expect any variant to achieve interim threshold goals for MFHBCF by the start of IOT&E, considering the recent decline in this metric over the past year. In fact, indications are that for each variant, this metric is the furthest from its current interim goal.

• Failing to grow reliability sufficiently by the start of IOT&E will make achieving the necessary 80 percent availability to accomplish all mission trials within the planned time span very difficult. Further, a failure to achieve adequate MFHBCF reliability in particular will impede the ability of the Operational Test Squadrons (OTS) to generate multiple four-ship formations with all required mission systems functional, a necessary condition for a set of the planned mission trials.

• A number of components have demonstrated reliability much lower than predicted by engineering analysis. This drives down the overall system reliability and can lead to long wait times for resupply as the field demands more spare parts than the program planned to provide. Aircraft availability is also negatively affected by longer-than-predicted component repair times. The table at top right shows some of the high-driver components affecting low availability and reliability, grouped by components common to all variants, followed by components failing more frequently on a particular variant or which are completely unique to it.

HIGH-DRIVER COMPONENTS AFFECTING LOW AVAILABILITY AND RELIABILITY

Variant	Common to All Variants	Additional High Drivers by Variant
F-35A	• Avionics Processors • Low Observable Maintenance • Shock Struts • Cold Air Duct • IPP Vent Fan Controller • Main Landing Gear Tires • Nutplates • On-Board Oxygen Generating System	• Horizontal Tail Actuation • Vertical Tail Bulb Seal • Electronic Warfare Receiver
F-35B		• Fuel System Components and Mods • Flexible Linear Shaped Charge
F-35C		• Main Landing Gear Retract Actuator * • Nose Landing Gear Steering Motor *

* Unique to the F-35C
IPP – Integrated Power Package

- The composition of the list of some of the high-driver components has changed as the program has progressed and either fielded more reliable components, or new failures have occurred to displace previous high drivers. For example, compared to the list reported in previous DOT&E Annual Reports, the 270V DC battery and associated components, the F-35B Upper Lift Fan Door Actuator, and the exhaust nozzle assembly components used on the F-35A and F-35C, are no longer high drivers. Improving aircraft availability can be realized by more than just improving the reliability of components and restocking supply with improved, redesigned parts; updating JTD and improving repair procedures can contribute to increased aircraft availability as well. However, in the current reporting period, overall reliability has not increased and new components have become high drivers, such as the Electronic Warfare Receiver and the Vertical Tail Bulb Seal. Note also that the program released Block 2B capabilities and flight envelope to the fleet in the period of this report. As the flight envelope is expanding and the fleet uses more mission system capabilities, new failure modes will likely emerge to dampen the overall effect of individual reliability improvements, consistent with recent trends observed in reliability growth analysis.

Maintainability

• The amount of time needed to repair aircraft and return them to flying status remains higher than the requirement for the system when mature, but has improved over the past year. The program assesses this time with several measures, including Mean Corrective Maintenance Time for Critical Failures (MCMTCF) and Mean Time To Repair (MTTR) for all unscheduled maintenance. MCMTCF measures active maintenance time to correct only the subset of failures that prevent the F-35 from being able to perform a specific mission; it indicates how long it takes, on average, for maintainers to return an aircraft from NMC to Mission Capable (MC) status. MTTR measures the average active maintenance time for all unscheduled maintenance actions; it is a general indicator of the ease and timeliness of repair.

Both measures include active touch labor time and cure times for coatings, sealants, paints, etc., but do not include logistics delay times, such as how long it takes to receive shipment of a replacement part.

- The tables below compare measured MCMTCF and MTTR values for the 3-month period ending in July 2016 to the ORD threshold and the percentage of the value to the threshold for all three variants. The tables also show the value from May 2015, the month reported in the FY15 DOT&E Annual Report, for reference. [Note that the May 2015 values may be different than those in the FY15 DOT&E Annual Report due to the revision of the scoring rules described at the beginning of the Reliability Growth section above.] For maintainability, lower repair times are better. Three of six metrics improved marginally, while three metrics, F-35B and F-35C MCMTCF, and F-35A MTTR, increased or worsened. Currently, all mean repair times are at least or nearly twice as long as their ORD threshold values for maturity, reflecting a heavy maintenance burden currently being carried by fielded units.

F-35 MAINTAINABILITY: MCMTCF (HOURS)				
Variant	ORD Threshold	Values as of July 31, 2016 (3 Mos. Rolling Window)	Observed Value as Percent of Threshold	Values as of May 2015 (3 Mos. Rolling Window)
F-35A	4.0	10.6	265%	11.4
F-35B	4.5	13.2	293%	12.7
F-35C	4.0	10.1	253%	8.4

F-35 MAINTAINABILITY: MTTR (HOURS)				
Variant	ORD Threshold	Values as of July 31, 2016 (3 Mos. Rolling Window)	Observed Value as Percent of Threshold	Values as of May 2015 (3 Mos. Rolling Window)
F-35A	2.5	6.3	252%	4.7
F-35B	3.0	7.3	243%	7.7
F-35C	2.5	4.9	196%	5.3

  - A more in-depth analysis of data from between August 2015 and July 2016, in order to capture longer-term 1-year trends, shows that for the MCMTCF metric, the F-35A and F-35B repair times are decreasing, while for the F-35C it is relatively flat. For overall mean repair times, however, the F-35A exhibited a slight increasing, or worsening trend; the F-35B showed a slight decreasing, or improving, trend; and the F-35C was relatively stable. Prior to May 2015, all six metrics were improving. In contrast, the more recent trend from this period generally indicates a slowing of improvement in the maintainability metrics.
  - All six maintainability metrics exhibit high month-to-month variability. Due to this variability, it is difficult to make projections in trends for maintenance metrics; however, it will be challenging for the program to meet the threshold values by maturity with the rate of improvement slowing and when current values for repair times are at least twice as high as requirements.
  - Several factors negatively influenced the ability to conduct quick and efficient maintenance. Extensive adhesive cure times for structural repairs, such as attaching hardware (e.g., nutplates and installing heat blankets around the engine bay), as well as long material cure times for low observable (LO) repairs, remain drivers. The cure time for some LO materials can be as high as 168 hours, for example, although units can accelerate this if they have appropriate tools.
  - Other factors that indirectly affect maintainability metrics have also been raised as concerns by maintainers. Maintainers must physically connect Portable Maintenance Aid (PMA) laptops to the aircraft in order to conduct most maintenance activities. The PMAs enable the maintainers to get status and configuration information from the aircraft, as well as control aircraft functions to enable other maintenance, such as opening the bomb bay doors where the cooling-air receptacle is located in order to apply air conditioning while running avionics on the ground. Maintainers also access the Anomaly Fault Resolution System (AFRS), which automatically troubleshoots Health Reporting Codes (HRCs) generated by the on-aircraft PHM system, and access JTD, which tells maintainers how to effect repairs identified by AFRS, via the PMA. Finally, maintainers record their work with the PMAs as well. However, synching the PMAs to the aircraft to conduct maintenance has been difficult, time-consuming and, in many instances, maintainers must attempt to synch several PMAs with an aircraft before finding one that will successfully connect. These connections are called Maintainer Vehicle Interface (MVI) sessions. Occasionally PMAs disconnect in the middle of an MVI session, which also hampers efficient maintenance. Recently, the program introduced improved MVI cable adapters to prevent accidental physical disconnection, which has helped. Software-related problems persist as well, such as PMAs taking anywhere from seconds to minutes to connect. This occasionally leads maintainers to disconnect a PMA they incorrectly believe is failing to connect, which prevents that PMA from connecting to an aircraft until an Automatic Logistics Information System (ALIS) administrator resets it, which can be a lengthy process.

- Maintainers have reported several difficulties with troubleshooting the aircraft, which is the first step in many maintenance actions. Normally, the aircraft PHM system produces HRCs and then maintainers use AFRS to identify possible root causes for those HRCs as well as determine the appropriate repair action. Often, AFRS will provide a "solution set," which lists several possible root causes for an HRC, rank ordered by probability of occurrence. While AFRS coverage is improving, it currently provides effective solution sets only approximately 70 percent of the time.

Particularly, when an aircraft fails a Vehicle Systems (VS) Built-In Test (BIT), an aircraft self-check conducted pre- and post-flight, there is no specific HRC produced, making these relatively frequent occurrences difficult to troubleshoot. When there is no HRC, such as in a VS BIT failure or manually reported fault, or AFRS does not produce a solution set for an HRC, or all the solutions offered by AFRS fail to resolve a fault, units must use other resources to troubleshoot the discrepancy. The primary method is to submit Action Requests (AR) to the joint JPO-Lockheed Martin Lightning Support Team (LST), whose engineers will further troubleshoot the aircraft remotely. The AR response times vary significantly, depending on category and urgency, but average several days to get a final response. Alternatively, or in conjunction, maintainers can use experience to troubleshoot on their own; however, in most cases they lack any system theory-of-operation or troubleshooting manuals that tell them how aircraft systems work. The current JTD are primarily dedicated to instructions only for repair actions for which AFRS has already identified a solution, and not for teaching maintainers the details of systems operations. Recently, the program and Lockheed Martin have started to provide some troubleshooting manuals to field maintainers for select mission systems to try to improve the poor fleet FMC performance. The extent to which these manuals will help troubleshooting and result in higher FMC rates remains to be determined.

- F-35 flying squadrons also have a heavy burden of scheduled maintenance. In particular, maintenance units have reported that daily servicing and inspection tasks, known as the Before-Operations Servicing (BOS), Inter-Operations Servicing (IOS), and Post-Operations Servicing (POS), are very time-consuming compared to similar inspections on legacy aircraft. Some of these daily inspections also require power and cooling air application on the aircraft, so a unit's ability to perform them is a function of the amount of Support Equipment (SE) assigned or available when needed. As the fleet matures and more data become available, the Services may be able to increase intervals between certain scheduled inspection tasks to reduce the man-hours that units must dedicate to this type of maintenance, if field experience warrants this. However, it is not clear the scheduled maintenance burden will reduce in the near future.

Autonomic Logistics Information System (ALIS)

- The program continues to fall behind in ALIS development and fielding. Although the program planned to test and field the next iteration of capability, designated ALIS 2.0.2, in 2016 to support the Air Force's decision to declare Initial Operational Capability (IOC) in August, the program failed to do so. Additionally, the program continued to defer planned content from ALIS 3.0 to post-SDD development.
- ALIS includes hardware and software that connects with all aspects of F-35 operations, including maintenance management, aircraft health, supply chain management, Offboard Mission Support (OMS) mission planning, along with tracking and management of pilot and maintainer training. Units rely on ALIS for planning and executing deployments by managing the data required to transfer aircraft, materiel, and personnel from home station to a deployed or expeditionary environment. Similar to the manner in which the program develops and fields mission systems capability in the air vehicle, it fields ALIS in increments.
  - The program fielded ALIS software version 2.0.1.1 in late 2015. Since that time, the program has released two updates, 2.0.1.2 and 2.0.1.3, to address previously identified, usability-related deficiencies. These software updates include fixes to existing deficiencies and usability problems, but do not add new capabilities to ALIS. Prior to the release of the first update with ALIS 2.0.1.2, the program attempted to field ALIS software versions with both new capabilities and deficiency corrections, a process which tended to add new problems while fixing some existing problems. Instead, the program now plans to continue fielding updates dedicated only to correcting deficiencies every three months until the release of ALIS 3.0, the final release scheduled for SDD.
  - Although the program had planned to field a new version of ALIS software, version 2.0.2, in the second half of 2016, in time to support the U.S. Air Force IOC declaration, it was unable to do so. ALIS 2.0.2 includes propulsion integration, a key capability the Air Force had planned to have for IOC; however, the Air Force declared IOC with ALIS 2.0.1 in August, forgoing those capabilities. Because the program continued to experience technical difficulties integrating propulsion functionality into ALIS, fielding of 2.0.2 slipped into CY17. As a result, operational units began 2016 with ALIS 2.0.1.1 and will finish the year with ALIS 2.0.1.3; receiving only updates to address deficiencies and without any additional capability fielded in ALIS.
  - Delays in ALIS 2.0.2 have affected the development of the next, and last, major release of ALIS software within SDD, ALIS 3.0, because Lockheed Martin shifted personnel from ALIS 3.0 development to support completing ALIS 2.0.2 development. Because the program can no longer complete ALIS 3.0 with all of the additional capability development planned by the end of SDD, it has restructured the planned ALIS increments for the remainder of SDD and for Follow-on Modernization (FoM). This restructuring reduces the content of ALIS 3.0 from earlier plans, defers content from ALIS 3.0 that the program has now determined is not required for IOT&E to post-SDD development, and also adds Service and partner priorities and emerging requirements for security updates. The resulting plan from the restructuring was to field four increments of software at 6-month intervals; the first, ALIS 3.0, scheduled to field in mid-to-late 2018, which is required for IOT&E, followed by the remaining three after SDD. These incremental software releases are also intended to resolve ALIS deficiencies and usability

problems. At the mid-point between each of these major releases, the program plans to deliver software updates to continue addressing usability problems and deficiencies. Because no fielding or Logistics Test and Evaluation (LT&E) events of additional ALIS capability have occurred for over a year, the program's plan to develop, test, and field these ALIS 3.0 and later versions appears overly ambitious with a low likelihood of actually being realized. Regardless of whether ALIS 3.0 or a later version has been fielded, or which capabilities are included, IOT&E will evaluate the suitability of the F-35 and ALIS in operationally realistic conditions.

- Until 2016, formal testing of ALIS software only took place at the Edwards AFB, California, flight test center on non-operationally representative ALIS hardware, which relied on reach-back capability to the Lockheed Martin facilities at Fort Worth, Texas. Although some formal testing will continue to occur in this manner, the program developed and fielded a dedicated end-to-end developmental testing venue for ALIS located in part at Edwards AFB and in part at Lockheed Martin in Fort Worth in 2016. This venue, referred to as the Operationally Representative Environment (ORE), reflects the end-to-end Autonomic Logistics infrastructure used to support fielded operations, including one Autonomic Logistics Operating Unit (ALOU), which represents the main hub at Lockheed Martin Fort Worth, two Central Points of Entry (CPEs), representing the country-unique portal from the main hub, and two Standard Operating Units (SOUs), representing squadron-level ALIS components, all networked together in a closed environment. Although the ORE provides for more realistic developmental testing of ALIS hardware and software for early problem discovery and fixing deficiencies, the current closed environment does not adequately represent the variety of ways in which the Services operate ALIS in different environments. ALIS testing at the flight test center is limited in several ways. First, the inability of ALIS to support their engines and lift fans, which differ from production models, so LT&E of propulsion functionality in ALIS cannot take place there. Also, the flight test center does not use ALIS capabilities routinely, such as Squadron Health Management (SHM), AFRS, or the Computerized Maintenance Management System (CMMS), as operational units do. Finally, the flight test center does not use PHM capabilities, as they are used by operational units, since the flight test aircraft have additional sensors and onboard instrumentation that provide the flight test center with more information than is available through PHM.

ALIS Software Testing and Fielding in 2016

- Although the program planned to test and field new capability with ALIS 2.0.2 software release in 2016, it failed to do so. The plans for added capability in ALIS 2.0.2 include:
  - Life Limited Parts Management (LLPM), which includes:
    - Propulsion integration. Currently propulsion data are downloaded from aircraft portable memory devices and provided to Pratt & Whitney Field Service Engineers for processing and generation of maintenance work orders. Propulsion integration will allow ALIS to process propulsion data in the same manner as aircraft data.
    - Production Aircraft Inspection Requirements (PAIRs). ALIS 2.0.2 will include the first phase of the PAIRs system. The program added PAIRs as part of the PHM after eliminating most of the originally planned prognostic algorithms. The program plans to include 8 prognostic algorithms in ALIS 2.0.2 and 8 in ALIS 3.0 out of the originally planned 128 SDD algorithms.
  - Sub-squadron reporting. This will allow the air vehicle to report its status back to the home squadron SOU even when it is deployed away from the majority of a squadron's assets.
  - SOU-to-SOU communication. Currently, information on one U.S. SOU is transferred to another by routing files from the originating SOU through the CPE at Eglin AFB, Florida, to the ALOU at Fort Worth, Texas, back through the CPE and to the receiving SOU. This new capability will permit targeted routing of files between SOUs under specific circumstances and is geared primarily toward making aircraft deployments more efficient.
  - Deployability improvements. This includes improved deployment planning and the bulk transfer of all deploying assets at once. The current release of ALIS makes deployment planning inefficient as it does not provide a centralized location in ALIS for this function. During deployments, squadrons currently transfer aircraft, supply, and support equipment data files individually.
  - Commercial Off-the-Shelf (COTS) hardware replacement. This allows the program to plan for hardware obsolescence and substitute newer hardware over time.
  - ALIS Readiness Check. Improves the health monitoring of ALIS processes.
- Testing of ALIS 2.0.2 will occur in multiple stages at multiple venues. The program plans to conduct an LT&E on the air vehicle portion of the ALIS 2.0.2 software package in early 2017, including initial testing of the propulsion module of the software in the ORE. Once those tests are complete, the program plans to do a validation and verification of the process to upgrade to ALIS 2.0.2, including the data migration, at an operational unit – possibly Luke AFB, Arizona – before fielding ALIS across the rest of the F-35 operating locations.
- Releasing ALIS 2.0.2 to field units will require significant manual intervention and data verification efforts to transition each site, which will likely affect flight operations. The data migration effort for ALIS 2.0.2 will be more complex and will take longer than previous ALIS releases because of propulsion integration and changes in data structures. For example, the Program Office noted that one ALIS domain alone, Customer Relationship Management, will require 40 man-hours for data migration and verification. Currently, the program estimates that each site will require 8 days

to complete the transition of all assets. Lockheed Martin will conduct the migration and has plans to complete the transition at each site by using the Friday through Monday time period of two consecutive weeks. Whether or not the affected squadron can continue flying operations between the two transition periods is unknown. As of September 2016, the program must transition 56 sites—either SOUs or CPEs—through this process. As of the time of this report, the program had not released a comprehensive transition plan.

Assessment of ALIS Support to Deployment Demonstrations with Operational Units

- Because of delays in ALIS release 2.0.2, fielded units have operated with ALIS 2.0.1 since October 2015. As planned, the Marine Corps used this release for a deployment demonstration to the Marine Corps Air Ground Combat Center (MCAGCC) Twentynine Palms, California, in December 2015, which DOT&E reported on in the FY15 DOT&E Annual Report. Similarly, the Air Force conducted a deployment demonstration to Mountain Home AFB, Idaho, in February 2016. The operational test squadrons from Edwards AFB participated in each of these demonstrations; however, the ALIS hardware came from operational units (a Marine Corps squadron from MCAS Yuma for the MCAGCC demonstration and an Air Force squadron from Hill AFB, Utah, for the Mountain Home demonstration).
- The Air Force completed its first F-35A deployment away from Edwards AFB, California, with six aircraft from the 31st Test and Evaluation Squadron (31TES) to Mountain Home AFB, which has no organic F-35 capability, from February 8 to March 2, 2016. All aircraft that participated in the deployment were in Block 2B configuration with software version 2BR5.2. This deployment was a Service-led assessment.
  - This deployment was the first time the Air Force deployed with a modularized, more transportable version of the ALIS hardware, referred to as SOU v2. ALIS software version 2.0.1 was used for this deployment, as well as for the Marine Corps' deployment to Twentynine Palms; the previous "cross ramp" deployment at Edwards AFB in May 2015 used the bulky SOU v1.[1] Deployed personnel had no difficulty setting up and configuring the ALIS network at Mountain Home AFB; however, they had a great deal of difficulty using ALIS on the local base network. After several days of troubleshooting, Information Technology (IT) personnel and ALIS administrators determined that they had to change several settings on the base network at Mountain Home and in the web interface application (i.e., Internet Explorer) to permit users to log on to ALIS. One of these changes involved lowering the security setting on the base network, an action that may not be compatible with required cybersecurity and network protection standards in place.
  - Data file transfers took place more quickly than in the previous F-35 deployment demonstrations, (i.e., the F-35A cross ramp deployment and the Marine Corps' deployment demonstration to MCAGCC Twentynine Palms). However, Lockheed Martin provided the five ALIS administrators normally assigned to the 31TES and three additional, highly experienced ALIS administrators from other locations to provide deployment support, more than for any previous deployment. Whether the Service's concept of operations for deploying ALIS will call for this level of ALIS administrative support, to ensure timely and accurate transfer of aircraft data at the deployed location, is still not known. Although the process was time-consuming and labor-intensive, they completed the transfer of all data to the deployed SOU v2 before deployed flight operations were scheduled to begin. To account for the expected extended time for data transfers, the 31TES allocated the ferry date and two additional days to complete the transfers; flight operations began on the third day of the deployment, as planned. Service deployment concepts of operations may need to account for time to transfer aircraft data files and ensure accuracy before beginning – or at least sustaining – operations at deployed locations.
  - Because of ambiguity in the ordnance loading technical data, one aircraft experienced major damage to a weapons bay door and horizontal tail early in the deployment when a bomb, which was incorrectly loaded, struck the aircraft following release. Aircraft repairs were extensive enough to require most of the remainder of the deployment to complete. The Marine Corps had previously discovered this ambiguity in the technical data, but the program did not disseminate this information across the F-35 enterprise.
  - Preparations to redeploy back to Edwards AFB began on March 1, 2016, with aircraft departing on March 2 and aircraft data file transfer from the deployed SOU beginning as soon as the aircraft took off from Mountain Home AFB. Though ALIS administrators transferred all data off the deployed SOU at Mountain Home AFB, administrators at Edwards AFB did not finish inducting aircraft files back onto the Edwards AFB SOU until March 4. The redeployed aircraft were ready for flight at Edwards on March 5, a 4-day transition period.
- Since the Services have not yet completed ALIS Concept of Operations (CONOPs) development, they will likely need to take into account the results of these deployments when determining the procedures and timing of F-35 deployments. Although the aircraft may be flown for short periods of time without ALIS, operational planners may need to allow for additional time between aircraft deployment and the beginning of deployed flight operations, compared to legacy

1. The 31st TES previously conducted a "cross ramp deployment" at its home base, Edwards AFB, from April 27 to May 8, 2015, to support deployment concept of operations development. DOT&E reported on this activity in the FY15 Annual Report.

platforms. Deployed operations, including the set-up and support from ALIS, will be evaluated during IOT&E.

- The challenges facing the Services and program in making ALIS deployable now involves software. Previously, the program identified the need to move from the bulkier, heavy SOU version 1 (v1) racks, which weighed approximately 1,600 pounds each, to the more customizable, modularized, two-man portable components in the SOU v2, so that the ALIS "footprint" could meet F-35 deployability requirements. Although the SOU v2 has improved the deployability of the ALIS hardware, these recent deployments show that lack of flexibility exhibited in integrating ALIS into new or existing networks, along with deficiencies in ALIS functionality and usability, contribute more to deployability problems than just the previously-identified hardware limitations.

ALIS Software and Hardware Development Planning from 2016 through the End of SDD

- In CY16, the program continued to struggle with providing the planned increments of capability to support the scheduled releases of ALIS software 2.0.2 to such an extent that the program now cannot accomplish the original plan for ALIS 3.0 development. As the objective date for Air Force IOC neared, the program considered releasing ALIS 2.0.2 in two increments: the first with all capabilities aside from propulsion integration in time to support an August 2016 Air Force IOC declaration; the second with propulsion integration, when the program overcame technical problems and completed formal testing. When the Air Force declared IOC without ALIS 2.0.2, using the already-fielded version of ALIS 2.0.1.3 instead, the need for a two-phase release no longer existed. As a result, the program now plans to conduct the LT&E of ALIS 2.0.2 in two parts in early 2017; the first with all functionality except propulsion integration at the flight test center, then propulsion integration in the ORE. ALIS 2.0.2 has been delayed for over a year from the release schedule approved in CY15.
- The Program Office planned for the release of ALIS 3.0 in June 2017, in time to support its planned start date for IOT&E, but now plans to release it in mid-to-late 2018. However, the ongoing delays with ALIS 2.0.2 and the resulting restructuring of ALIS 3.0 and beyond, have caused the program to defer capability that had been planned to be delivered with ALIS 3.0. The following list includes major capabilities the program planned for ALIS 3.0 inclusion, and identifies which ones are now being deferred – in full or in part – out of SDD:
  - Decentralized maintenance. This will enable execution of the sortie generation cycle with a deployable PMA for independent maintenance workflow while maintainers work in the shadow of the aircraft. Decentralized maintenance is now divided into two parts, both deferred to post-SDD software versions.
  - Resource sharing. This capability will allow the sharing of tools, support equipment, pilots, and training records across squadrons without requiring the transfer of data between SOUs. Deferred to post-SDD software release.
  - Security enhancements. This includes additional ALIS readiness checks to validate and monitor user accounts and additional penetration testing.
  - Offboard Prognostic Health Management (PHM). Additional algorithms to assess materiel condition independently of ALIS releases and to implement a correlation function between the Integrated Caution, Advisory and Warning (ICAW) system and HRCs. Partially deferred to post-SDD software release; only 16 of 128 planned prognostic algorithms are now included within SDD.
  - Life Limited Parts Management (phase 2). Adds an Identify Locate (IDLO) viewer for product life-cycle management, support for lightning protection and On-Board Inert Gas Generation System (OBIGGS), Illustrated Parts Breakdown product, Complex PAIRs to manage remaining life of aircraft components, support for quick engine changes, the HMDS, and back-shop visibility for supply chain management. Full Life Limited Parts Management in ALIS was a capability the program originally planned for ALIS 2.0.0 to support Marine Corps IOC; however, the re-baselining of this technically difficult-to-implement capability has resulted in it not being fielded for at least 2 years after IOC declaration.
  - COTS hardware replacement.
  - Corrosion Management System. Will improve the ability of ALIS to track and report the corrosion conditions of aircraft using two sensors located in designated positions within the aircraft and includes corrosion HRCs in ALIS. Deferred to post-SDD software release.
  - Low Observable Health Assessment System (LOHAS) enhancements. Partially deferred to post-SDD release.

Prognostic Health Management (PHM) within ALIS

- The PHM system is designed to collect performance data to determine the operational status of the air vehicle and, upon reaching maturity, will use data collected across the F-35 enterprise and stored within PHM to predict maintenance requirements based on trends. The PHM system is designed to provide the capability to diagnose and isolate failures, track and trend the health and life of components, and enable autonomic logistics using air vehicle HRCs collected during flight and saved on aircraft PMDs. The F-35 PHM system has three major components: fault and failure management (diagnostic capability), life and usage management (prognostic capability), and data management. PHM diagnostic and data management capabilities remain immature. The program has yet to integrate any prognostic capabilities; the first set of algorithms is planned for ALIS 2.0.2.
- Diagnostic capability should detect true faults within the air vehicle and accurately isolate those faults to a line replaceable component. However, to date, F-35 diagnostic capabilities continue to demonstrate poor accuracy, low

detection rates, and also have high false alarm rates. Although coverage of the fault detection has grown with the fielding of each Block of F-35 capability, all metrics of performance remain below threshold requirements. The table below compares specific diagnostic measures from the ORD with current values of performance through April 2016.

- PHM monitors nearly every on- and offboard system on the F-35. It must be highly integrated to function as intended and requires continuous improvements for the system to mature.
- Poor diagnostic performance increases maintenance downtime. Maintainers often conduct BITs to see if the fault codes detected by the diagnostics are true faults. False failures (diagnostics detecting a failure when one does not exist) require Service personnel to conduct unnecessary maintenance actions and often rely on contractor support to diagnose system faults more accurately. These actions increase maintenance man-hours per flight hour, which in turn can reduce aircraft availability rates and sortie generation rates. Poor accuracy of diagnostic tools can also lead to desensitizing maintenance personnel to actual faults.
- The number of false alarms recorded within ALIS can be artificially lowered, as qualified maintenance supervisors can defer or cancel an HRC without generating a work order for maintenance actions, if they know that the HRC corresponds to a false alarm not yet added to the nuisance filter list. The deferred or canceled HRC will not result in the generation of a work order, and it will not count as a false alarm in the metrics in the table below. The program does not score an HRC as a false alarm unless a maintainer signs off a work order indicating that the problem described by the HRC did not occur. Because PHM is immature and this course of action saves time for the maintainers, it occurs regularly at field locations; however, this means the number of recorded false alarms is not always an accurate reflection of the HRC false alarm rate.
- Comparing the values in the table below with those in the FY15 DOT&E Annual Report shows improvement in Fault Detection Coverage, Fault Detection Rate, Fault Isolation Rate for non-electronic faults to one Line Replaceable Component (LRC), and – most significantly – Mean Flight Hours Between Safety Critical False Alarms. Mean Flight Hours Between False Alarms and Fault Isolation Rate for non-electronic faults to three or fewer LRCs show no significant improvement, and Fault Isolation Rate for electronic faults to one LRC has gotten worse since last year's report. At this time, Mean Flight Hours Between Flight Safety Critical False Alarm and Fault Isolation Rate for non-electronic faults to one LRC are the only diagnostic metrics which appear to be improving adequately toward meeting their threshold requirements. The program planned for accurate diagnostics to support a planned level of sustainment; poor diagnostics contribute to poor reliability and maintainability metrics, reducing aircraft availability and increasing aircraft downtime.
- Following are the systems most likely to result in missed fault detections, incorrect fault isolations, and false alarms as of April 2016.
  - Missed detections: Integrated Core Processor (ICP), Communications, Navigation, and Identification (CNI) rack modules, Panoramic Cockpit Display, Power and Thermal Management System (PTMS), and vehicle system processing.
  - Incorrect isolation: ICP, PTMS, EW, electric power, and hydraulic power system.
  - False alarms: Propulsion, CNI system, EW, ICP, and displays and indicators in general.
- The Program Office initiated a PHM maturation plan in 2015 to improve the performance of each of the three major components of PHM:
  - Improving BIT functionality, PHM software handling of BIT results, and off-aircraft filter lists and fault isolation instructions; also focusing on identified high-fault drivers to prioritize developing AFRS solutions with the greatest impact on fault detection and isolation, false alarm

METRICS OF DIAGNOSTIC CAPABILITY
(6-month rolling window as of April 2016. Data provided by Program Office considered "preliminary" as they have not completed formal adjudication process by the data review board.)

Diagnostic Measure	Threshold Requirement	Demonstrated Performance		
		Block 1	Block 2	Block 3
Developmental Test and Production Aircraft				
Fault Detection Coverage (percent mission critical failures detectable by PHM)	N/A	88	88	93
Fault Detection Rate (percent correct detections for detectable failures)	98	88	88	93
Fault Isolation Rate (percentage): Electronic Fault to One Line Replaceable Component (LRC)	90	65	64	42
Fault Isolation Rate (percentage): Non-Electronic Fault to One LRC	70	71	73	86
Fault Isolate Rate (percentage): Non-Electronic Fault to Three or Fewer LRCs	90	87	87	100
Production Aircraft Only				
Mean Flight Hours Between False Alarms	50	0.09	0.41	0.50
Mean Flight Hours Between Flight Safety Critical False Alarms	450	61	537	437
Accumulated Flight Hours for Measures	N/A	61	6,440	6,111
Ratio of False Alarms to Valid Maintenance Events	N/A	135:1	19:1	19:1

performance, unnecessary maintenance, high maintenance man-hours, aircraft availability, and excess cost
  - Improving the functionality of PAIRS and algorithms which assess materiel condition based on usage and repair feedback, potentially adding new life tracking items based on fleet experience
  - Improving or adding data collection from the air vehicle, improving data downloading and processing from the aircraft to ALIS, and improving distribution and storage of data to better support user needs
- Structural PHM (SPHM) is a key element of overall airframe life-cycle management. It includes conditional event detection and analysis, including over-g, hard landing, overspeed, and overload conditions, and is planned to provide a corrosion monitoring and predictive modeling capability. The air vehicle currently includes two corrosion sensors—one on the forward face of the radome bulkhead and the other on the wall of the bay housing the fuel/heat exchanger. ALIS 2.0.0 included a logging function for these corrosion sensors. A Program Office study completed in November 2015 determined that 27 percent of the corrosion sensors in the fleet had failed, so the program is in the process of developing a new sensor manufactured with more precise sealing applications to be used during production instead of upon installation.

Air-Ship Integration and Ship Suitability Testing

F-35B

- The integrated test team from Patuxent River, Maryland, conducted the third and final planned set of F-35B ship trials, referred to as Developmental Test III (DT-III), from October 28 through November 17, 2016, on USS *America*. The objectives for this 3-week developmental test event included:
  - Expanding the vertical landing flight envelope for both day and night operations (higher wind-over-deck conditions and operations at higher sea states than earlier ship trials, as well as operating from additional landing spots farther forward on the flight deck)
  - Evaluating the Gen III HMDS for nighttime landings, with or without landing aids on the ship
  - Assessing Joint Precision Approach Landing System (JPALS) functionality
  - Conducting vertical landings and short take-offs with symmetric and asymmetric external loads carriage
  - Expanding vertical take-off capability
  - Evaluating environmental effects from flight operations, such as the thermal tolerance and response of the flight deck to vertical landings and noise surveys from various ship locations
  - Conducting maintenance demonstrations – including engine and lift fan removal and replacement actions, and a power module maintenance demonstration – and loading and unloading of external stores
  - Evaluating the operational capability of the first deployment of an ALIS SOU v2 on the ship
- Besides the two developmental test aircraft from the Patuxent River test force (BF-1 and BF-5), the Marine Corps also supported the test activities by providing an additional three instrumented operational test aircraft assigned to VMX-1, the operational test unit at Edwards AFB, California, and two fleet aircraft from VMFA-211, one of the two operational units at MCAS Yuma, Arizona. Although primarily a developmental test event, the Marine Corps embarked fleet and operational test squadron personnel for training, and to inform the JSF Ship Integration Team in preparation for the first operational F-35B deployment onboard USS *Wasp*, planned for late 2017. From November 17 – 21, the Marine Corps also conducted a "Lightning Carrier" proof of concept demonstration, with an additional five F-35B fleet aircraft plus two MV-22 and two H-1 Air Combat Element (ACE) assets deployed to the ship to assess interoperability and the suitability of F-35B "Heavy" ACE configurations on LHA-class ships. Observations from this testing included:
  - The specialized secure space set aside for F-35-specific mission planning and the required Offboard Mission Support (OMS) workstations is likely too small and therefore unsuitable for regular ACE operations with the standard complement of six F-35B aircraft – let alone F-35B Heavy ACE configurations with more aircraft. Due to the classification of certain F-35 capabilities, pilots must conduct mission planning in a secure space. The ALIS SOU v2, which has several classified components, was also located in this space. However, pilots, the ALIS administrator, and security personnel commented that the compartment designated for the secure workspace onboard USS *America* was too small to accommodate enough OMS workstations and a sufficient briefing and debriefing area. Marine Corps and ship personnel are investigating using this compartment for ALIS only, and designating an alternate compartment for mission planning.
  - The power module maintenance demonstration was intended to show that a deployed unit could conduct modular engine maintenance at-sea. The F135 engine is modular, with a fan and compressor section; a power section with the combustion chamber and turbine stages; an afterburner section, which on the F-35B consists of a Three-Bearing Swivel Module (3BSM) that can rotate downward to more than 90 degrees for vertical flight; and a nozzle section. The general maintenance concept for a failed engine is to replace only the defective module on any given engine to return the overall engine to service more quickly, and send the defective module to depot-level repair. The demonstration consisted of splitting open an F135 engine mounted on two aligned Maintenance and Transportation Trailers (MTTs) into its modularized sections, removing a "bad" power module, taking a "good" spare power module out of its shipping and storage container, placing the good module into the

engine, and containerizing the bad module, all with the use of an overhead bridge crane in the aft high bay of the hangar bay. The demonstration showed that maintainers could swap a module at sea; however, the evolution took up a large amount of space in the hangar bay and occurred without a full ACE onboard. The Navy and Marine Corps should conduct some further analyses, such as an operational logistics footprint study which simulates flight deck and hangar bay spotting with a full ACE onboard, using data from this evolution to determine what the impact of this maintenance would be on integrated ship and ACE operations with a full ACE onboard.

- The detachment planned to stage an F135 engine removal and installation (R&I) demonstration, but early in the deployment maintainers discovered, during a Post-Operations Servicing, that one of the OT aircraft (BF-20) had a thrust pin that had unseated. There are several thrust attachments between the engine and the airframe that transfer the propulsive forces produced by the engine to the airframe, and this was the first time in program history that maintainers discovered a thrust pin had backed out of full engagement, a serious safety of flight concern. As a result, the unit submitted an AR to request disposition. The AR response directed that the engine be removed from the aircraft, and the thrust pin attachment points on both the engine and airframe be thoroughly inspected. This provided a natural opportunity to evaluate an actual engine R&I as opposed to a staged demonstration. The unit provided photos and dimensional data to the Lightning Support Team (LST), initiating a long investigation process to determine the root cause, but there were no immediately obvious signs of wear or damage. The LST eventually directed the squadron to replace the engine, as there was a full spare engine onboard, and the lift fan drive shaft. The squadron completed this maintenance in the hangar bay and, on November 16, conducted a High-Speed Low-Thrust (HSLT) engine operation on the flight deck to confirm that the new engine was installed correctly and fully functional. The unusual circumstances of this event primarily drove the 2-week long R&I process, as opposed to specific shipboard conditions and, by the time of this report, the program had not yet determined a root cause. However, the engine R&I was practically aided by the fact that, for this detachment, a full spare engine was available for immediate installation. Currently, the program's planned Afloat Spares Package of spare parts that will be loaded onboard the USS *Wasp* for the first F-35B deployment in 2017 will not have a full spare engine, only spare propulsion modules. See the F-35C ship suitability section for further details on F135 engine R&I concerns at sea.
- The squadron also conducted a staged lift-fan R&I demonstration on BF-20 while it was in an NMC status in the hangar bay for the engine R&I. Maintainers positioned the aircraft along the ship's centerline and directly beneath the bridge crane in the forward of two high bays. Organic Marine squadron personnel first used a collapsible, portable floor crane and an assembled support frame to cradle the upper lift fan door and remove it from the aircraft, and then place it on the deck. After maintainers attached another assembled frame to the top and sides of the lift fan, ship personnel used the overhead bridge crane to raise the lift fan out of the aircraft cavity and, via attached tether ropes to each of the four top corners of the frame to guide the lift fan, lowered it to a support cradle on the deck. Service personnel then reversed this process to reinstall the lift fan. After the upper lift fan door was reinstalled and maintainers were disassembling the support frame that attaches the door to the crane, a portion of this assembly fell onto the lift fan, damaging a stator strut at the top of the lift fan. Repairs to this strut took another couple of days to complete. Maintenance personnel noted several improvements that should be incorporated into this process; most importantly, the tether points for the lift fan support assembly need to be moved to the bottom four corners for better control, as the tethers provided very little control near the hook point of the crane; also the program should provide a protective maintenance cover for the lift fan to prevent damage during future lift fan R&I's or upper lift fan door maintenance.
- On November 15 and 16, a single fleet aircraft from VMFA-211 departed from USS *America* to drop live ordnance on targets on an inland range, hot-pitted for fuel from MCAS Yuma, Arizona, and returned to the ship each day. Both sorties dropped one GBU-12 laser-guided bomb and one GBU-32 JDAM. The Marine Corps originally intended to fly two loaded aircraft each day, but the lack of available mission-capable aircraft drove the detachment to launch only a single aircraft each day.
- While the set of sea trials were not focused on operational realism, several aspects were more operationally representative than the 2015 F-35B deployment demonstration onboard USS *Wasp*. The aircraft had a full suite of Block 2B electronic mission systems installed, unlike onboard USS *Wasp*; however, like the USS *Wasp* demonstration, these aircraft mission systems were not maintained to a full combat-mission-capable state of readiness. Unlike in 2015, the OT and fleet aircraft were cleared to carry live ordnance on the flight deck, with some workarounds. With this clearance, the test team intended to employ live ordnance on missions. Production-representative support equipment (SE) was onboard ship for the first time as well for use on the non-DT aircraft. Similar to the 2015 demonstration, the operational logistics support system, known as the Autonomic Logistics Global Sustainment system, was still not available. As a result, spares provisioning and supply support were not necessarily the same as would be expected on a combat deployment.

F-35C

- The third and final phase of F-35C ship suitability testing, designated Developmental Test III (DT-III), was conducted by VX-23, the developmental test team from Patuxent River, from August 10 – 26, 2016, aboard USS *George Washington*. The primary objective of DT-III was to complete characterization of the flying qualities of the F-35C aircraft for catapult launches and arrested recoveries, building on the results from two previous at-sea developmental test periods. The test team explored aircraft flight operations around the carrier in high crosswind conditions and, for the first time, with external ordnance, including asymmetric load-outs. Both day and night operations were conducted, allowing for assessments of the Gen III HMDS for night approaches and landings under varying light conditions. These investigations will help develop aircraft launch and recovery bulletins to an expanded envelope to support fleet operations. Also, while the ship was underway, VFA-101, the Navy's F-35C training squadron at Eglin AFB, Florida, participated in the event for other test objectives, including a Commander of Naval Air Forces (CNAF)-directed proof-of-concept demonstration of an F-35C engine R&I in the ship's hangar bay as well as initial day carrier qualifications for 12 pilots that would assess overall suitability of catapult launches and the Delta Flight Path capability for carrier approaches and landings.

- Initially, only developmental test aircraft CF-3 and CF-5 (transient aircraft needed for logistical support) and search and rescue helicopters deployed to the carrier. No air wing was present. Five VFA-101 aircraft deployed onboard the ship from August 14 – 18. The major contractor and test team were responsible for maintenance of CF-3 and CF-5, although fleet maintenance personnel supported the VFA-101 carrier qualifications and the engine R&I demonstration. ALIS was not installed on the carrier; it was accessed via satellite link to a location ashore.
- The developmental test team conducted night operations with modifications to the Helmet Display Unit for the Gen III HMDS that permitted lower illumination settings, intended to reduce the amount of "green glow" in the helmet display that makes seeing the lights on the carrier difficult during night operations. The test pilots reported that the refined brightness control somewhat improved the night carrier approaches; however, "green glow" was still a significant problem and is the subject of two Category 1 deficiency reports.
- From the carrier qualifications, the VFA-101 pilots found the F-35C catapult shot not operationally suitable due to excessive vertical (Nz) oscillations during launch. Although numerous deficiencies have been written against the F-35C catapult shot oscillations – starting with the initial set of F-35C ship trials (DT-I) in November 2014 – the deficiencies were considered acceptable for continued developmental testing. The fleet pilots reported that the oscillations were so severe that they could not read flight critical data, an unacceptable and unsafe situation during a critical phase of flight. Most of the pilots locked their harness during the catapult shot, which made emergency switches hard to reach, again creating an unacceptable and unsafe situation.
- The VFA-101 pilots reported that the Delta Flight Path mode of operation made carrier approaches easier on pilot workload and touchdown points more consistent. During the qualifications, pilots made 154 approaches and landings with 100 percent boarding rate and no bolters.
- The engine R&I proof-of-concept demonstration took 55 hours to complete and used about one-third to one-half of one of the three hangar bay partitions; this is much more space than that needed for an F/A-18 engine change. Because it was the first F-35C engine R&I demo at-sea, maintainers moved through all required steps at a slow pace to ensure safety first, which may have extended the timeline relative to what an experienced crew could achieve during routine maintenance operations. On the other hand, the maintainers had practically free use of most of the hangar bay space, which may have facilitated speedier maintenance relative to conducting an engine R&I with a full air wing onboard. As a result, actual engine R&I's during deployments may not differ drastically in time from this demonstration.
- While the proof-of-concept demonstration showed that an engine could physically be swapped at sea, it also revealed that such a major maintenance evolution would be very difficult, time consuming, take up a large amount of space, and be a drastic change from the engine R&I on legacy aircraft. The F-35C engine change is also more labor- and space-intensive than the F-35B engine R&I, such as conducted onboard the USS *America*. The F-35B engine R&I is aided by the aircraft's 3BSM doors, which open during regular operation to enable the exhaust nozzle to rotate downward to more than 90 degrees for vertical flight. Opening these doors for engine maintenance avoids the need to remove fixed panels, such as on the F-35A and F-35C. For the F-35C, many more skin panels and a large piece of structure known as the tail hook trestle, although not the tail hook itself, must be removed for an engine R&I. Storing these items, and the associated tubes and wire harnesses, so they will not be damaged while off the aircraft, also takes up additional space. The fact that the demonstration was conducted without a full air wing on the ship additionally limited the test team's ability to assess the likely impact of an F-35C engine change on integrated carrier-air wing operations. Such an assessment will be needed for IOT&E. Because of the complexity and time required to conduct an engine change, the Navy and JPO should investigate alternatives for determining the impact of an R&I while conducting carrier-air wing operations as well as improving the maintainability of the F-35 system at sea.

• Both the F-35B engine R&I onboard USS *America* and the F-35C engine R&I onboard USS *George Washington* were hampered by the lack of suitable strut locks approved for at-sea use, considering the rolling and pitching motion that may be experienced while underway. Since the engine is a significant part of the aircraft weight, without strut locks the airframe would raise up on the pressurized landing gear struts as soon as the engine was detached. This could potentially damage either the engine or airframe due to tight tolerances, or injure maintainers with hands in the area. In both cases, maintainers put the aircraft up on jacks to de-service the struts before the engine change, and then raised the aircraft back up on jacks to re-service the struts after the change, adding significant time to the process. Further, ship maneuvering is restricted when raising and lowering aircraft on jacks; engine R&I times could be decreased if the program develops, and the Navy approves, appropriate strut locks for at-sea use.

- Maintainers conducted a less extensive power module maintenance demonstration onboard USS *George Washington* than the one performed on USS *America*, consisting of removing a power module from its container in the hangar bay, moving it to the engine repair shop aft of the hangar bay, and returning it to its container. To open the container, maintainers used a motorized, wheeled, mobile crane that is part of the ship's SE complement to raise the container lid, which is composed of the roof and four side walls, over the encapsulated power module, and set it to the side in the hangar bay. A specialized Electric Pallet Jack (EPJ) was then used to move the power module, still attached to the container bottom, to the engine repair shop, where it could be transferred to an MTT via an overhead bridge crane. Maintainers expressed dissatisfaction with the container design, which required a large amount of space and a large piece of SE to remove, and stated that, while suspended on a possibly pitching and rolling ship, such a heavy item could present a safety hazard. They stated a preference for the type of container used for the T56 engine, installed on the E-2 Hawkeye and C-2 Greyhound aircraft. This type of container has a door on one side that opens outward, with the engine mounted on rails inside. An MTT can be wheeled up to the container and the engine slid onto it by hand. This configuration takes up less space to remove an engine, doesn't require any SE, is quicker, and presents fewer hazards. The current container is designed to a very high standard of structural integrity in order to withstand a fall if ever resupplied by moving it across a wire strung between a resupply ship and a carrier, a standard form of resupply at sea. However, only the planned heavy E-Stream wire system was capable of moving the heavy power module container, but this program is now canceled. The Navy now plans to resupply un-containerized power modules via internal carriage on a CV-22 aircraft, and containerize any spare modules onboard ship if needed for storage. The program and the Navy should investigate if the heavy power module container should be redesigned for better usability at sea.
- Current program plans do not provide a full spare engine for the envisioned Afloat Spares Package of parts that will go onboard Navy CVN and L-class ships to support F-35C and F-35B squadrons, respectively. This will significantly increase the amount of time required to conduct an actual engine change. The 55-hour timeline measured during the proof-of-concept demonstration provided above assumed a full spare engine ready for immediate install once the down engine is removed from the aircraft. Without a spare, the time required to troubleshoot the down engine to a bad module, disassemble the engine to swap that module, and then reassemble the engine to reinstall it into the aircraft must be added to the overall process; this can easily add several more days of downtime to the affected aircraft. Further, the probability of Foreign Object Damage (FOD) to engines is higher at sea than ashore, which may drive more frequent engine R&Is at sea. This is due to the close proximity of aircraft maintenance to the ship landing areas allowing foreign objects to migrate, and the more stressing arrested or vertical landings at sea, which can increase the probability of items like fasteners falling off an aircraft into the landing area.
- Access to ALIS offboard the ship via the ship's satellite communications was intermittent and troublesome, making transmitting large file sizes difficult. For example, a 200 MB file required 2 days to successfully transfer due to bandwidth limitations and inconsistent connectivity. These issues drove VFA-101 to operate in an ALIS offline mode for the majority of the detachment. While the root cause appeared to be due to limitations with the shipboard communications equipment vice ALIS directly, and deployed units will have an SOU onboard ship, the SOU will occasionally have to transmit large files to the CPE due to how data-intensive ALIS is. This requirement to communicate large amounts of information will likely be exacerbated after a ship emerges from a restricted Emissions Control (EMCON) period where transmissions from the ship are severely limited or cut-off completely. The program and the Navy should investigate potential options to improve ship-based communications bandwidth dedicated to ALIS connectivity off-ship, such as increasing the priority of ALIS transmissions, or reserving low-use times of the day for transmitting large volumes of ALIS message traffic.
- VFA-101 brought a suite of production-representative SE to the aircraft carrier, including electrically powered hydraulic, air conditioning, and polyalphaolefin (PAO) carts for use in the hangar bay. Personnel use the PAO cart to service the aircraft with this special fluid that cools the radar and some other avionics. The Navy prefers that SE for use in hangar bays be electrical vice diesel powered because of the enclosed environment. They also brought an engine R&I trailer and an engine maintenance trailer, needed for the engine maintenance demo. Collectively, these items of SE were larger than legacy items and took up a large amount of deck space. Hangar bay personnel commented that the size of the SE would also make them more difficult to move around a crowded hangar bay with a full air wing onboard. The Navy should investigate any efficient, multi-use opportunities for F-35 SE, such as using legacy SE on the F-35 or F-35 SE on legacy aircraft, to try to limit the impact on the overall SE footprint for an air wing with F-35

included. Additionally, the JOTT will evaluate SE operation and movement around the flight deck and hangar bay during IOT&E.

- Since the hangar-bay SE items are electrical, they rely on 440V power from outlets in the walls of the ship. Maintenance on a single F-35C can sometimes require external power, provided by a small transformer power cart that converts the 440V wall power to the 270V and 28V DC power used by the aircraft, along with air conditioning and hydraulic power, each requiring separate carts. Such maintenance activities would require the use of three wall outlets. However, most hangar bay partitions had four outlets, which would make simultaneous maintenance on more than one F-35C in a partition a coordination challenge. The Navy should investigate options for increasing the number of wall power outlets in hangar bays to help facilitate simultaneous maintenance on multiple F-35Cs, or the ability to interconnect multiple pieces of support equipment from a single outlet to permit simultaneous operations.
- The Navy is working on the following air-ship integration issues, primarily for carrier operations. Some of the following issues also apply to F-35B operations on L-class ships:
  - Flight deck Jet Blast Deflectors (JBDs) will require additional side panel cooling in order to withstand regular, cyclic limited afterburner use, during F-35C catapult launches. JBDs are retractable panels that redirect hot engine exhaust up and away from the rest of the flight deck when an aircraft is at high thrust for take-off. During IOT&E, an F-35C detachment will deploy to a CVN to evaluate sortie generation rate capability within an air wing context. The CVN used for IOT&E must have additional side panel cooling installed in the JBDs to enable the most operationally representative test to evaluate this Key Performance Parameter of the F-35C.
  - The Navy continues to procure a replacement mobile Material Handling Equipment crane for several purposes onboard carriers, including lifting the power module container lid as described above. This crane will only be used on CVNs, for F-35 maintenance only, as they lack the hangar-bay overhead cranes that L-class ships come equipped with. Since the FY15 DOT&E Annual Report, the crane acquisition has proceeded at a pace such that sufficient articles should be in the fleet in order to support a first F-35C deployment in the 2020 timeframe.
  - Two methods of shipboard aircraft firefighting for the F-35 with ordnance in the weapons bays are being developed, one for doors open and one for doors closed. Each method will use an adapter that can fit to the nozzle of a standard hose. The open door adapter will also attach to a 24-foot aircraft tow bar so firefighters can slide it underneath the aircraft and spray cooling water up into the bay. Development of this open door adapter is proceeding well and it was deployed to the USS *America* to support live ordnance carry by the OT and fleet F-35B aircraft during DT-III. However, the closed bay adapter, which intends to use water pressure to drive a saw to cut into the aircraft and lock a hose in place to douse a loaded weapons bay during a flight deck fire, was not yet ready for deployment. As a workaround, F-35B aircraft on USS *America* with live ordnance taxied with their weapons bay doors open, closing them only right before take-off, to mitigate the risk, but this will not be a standard practice for combat deployments.

Cybersecurity Operational Testing

- The JOTT continued to accomplish testing based on the cybersecurity strategy approved by DOT&E in February 2015, with some modifications due to test limitations, discussed below. In accordance with this strategy, in FY16 the JOTT conducted adversarial assessments (AA) of the ALIS 2.0.1 Squadron Kit and Central Point of Entry (CPE), completing testing that began in Fall 2015, and conducted cooperative vulnerability and penetration assessments (CVPA) of the mission systems Autonomic Logistics Operating Unit (ALOU) used to support developmental testing (referred to as the DT-ALOU), and the operational ALOU. The JOTT also completed a limited cybersecurity assessment of the F-35 air vehicle. These tests were not conducted concurrently as originally planned; therefore, end-to-end testing of ALIS, from the ALOU to the air vehicle, has not yet been accomplished. The JOTT initially tested the DT-ALOU in lieu of the operational ALOU because the JPO did not approve an Interim Authority to Test for the ALOU due to concerns that cybersecurity testing would adversely affect the ALOU's operations; however, a limited test of the operational ALOU was completed in October 2016 and an AA was scheduled for December 5 – 9, 2016.
  - The U.S. Navy's Commander, Operational Test and Evaluation Force (COTF) conducted a CVPA and limited AA against the DT-ALOU, from April 1 – 15, 2016, at Lockheed Martin's Fort Worth facility. The COTF testing verified that the DT-ALOU, configured with ALIS 2.0.1.3, had mitigated several key vulnerabilities discovered on ALIS 2.0.1.1 systems during fall 2015 testing. However, this testing of the DT-ALOU was not operationally representative because several key systems and external interfaces, from which cyber-attacks might originate, were not present. The testing was further constrained because the Program Office and Lockheed Martin only permitted testing to occur during overnight hours while the DT-ALOU was disconnected from external networks to minimize interference with operations. The COTF testing still discovered several minor security problems with the DT-ALOU. The operational ALOU is still configured with ALIS 2.0.1.1.
  - The U.S. Marine Corps Information Assurance Red Team (MCIART) conducted an AA of the Marine Fighter Attack Squadron 211 (VMFA-211) ALIS 2.0.1.3 Squadron Kit at Marine Corps Air Station Yuma, Arizona, April 25 through May 6, 2016. The unit's Squadron Kit was in the process of being stood up, so it was not in a fully operational configuration during the test. The operational

VMA-121 Squadron Kit was declared off-limits by Marine Corps personnel. MCIART verified that several key vulnerabilities discovered during the 2015 Squadron Kit testing had been mitigated; however, MCIART discovered several new vulnerabilities from insider and outsider threat postures.

- The U.S. Air Force 177th Information Aggressor Squadron (IAS) conducted an AA against the ALIS 2.0.1.3 Central Point of Entry (CPE) at Eglin AFB, Florida, from June 2 – 10, 2016. The 177 IAS assessed the system as an outsider and near-sider threat, and discovered vulnerabilities with various components of the CPE, despite the fact that Lockheed Martin administrators and ALIS users had implemented new operating procedures during the test to improve the CPE security posture.[2] The CPE classified servers were not adequately assessed due to time constraints and a lack of approval for connecting 177 IAS equipment to the classified CPE network.
- The JOTT, with support from the Air Force Research Laboratory (AFRL), conducted a limited CVPA of the F-35A Block 2B air vehicle, from September 26 – 27, 2016, at Edwards AFB, California. The CVPA tested the process by which the air vehicle validates the digital signature of files within the operational flight program when it is loaded onto the aircraft via the aircraft media device. This test was one of the test cases proposed by cybersecurity subject matter experts, and was the first cybersecurity assessment of an operational F-35 air vehicle. The successful accomplishment of this initial test should encourage the Program Office to examine other planned test cases in future air vehicle cybersecurity assessments. Analyses of the test results are ongoing.
- The COTF and the JOTT conducted a CVPA of the operational ALOU October 17 – 28, 2016, at Lockheed Martin's Fort Worth facility. The test team was augmented by Lockheed Martin Red Team members so that the ALOU could be examined for vulnerabilities from the Lockheed Martin Intranet (LMI). COTF and the JOTT were not permitted to conduct any test activities on the ALOU unless it was disconnected from the LMI, limiting the operational realism of the test and precluding certain vulnerabilities from being assessed. Detailed analyses of the data collected are ongoing.

- In response to DOT&E's recommendation that active intrusion discovery and forensics, referred to as a Blue Hunt, be conducted on the Squadron Kit and CPE, the JOTT has scheduled the 855th Cyber Protection Team (CPT) to conduct two events for the end of CY16. Current plans are to perform mostly vulnerability assessment and traditional Red Team activities against these systems —not active intrusion discovery and forensics—and so it is still unclear whether these events will fulfill DOT&E's request. Additionally, the JOTT will need to conduct a Blue Hunt on the ALOU once ALIS 2.0.2.4 is loaded and then additional Blue Hunts on all ALIS levels (ALOU, CPE, and Squadron Kit) each time a full increment of ALIS software is released.
- While progress towards fulfilling missed test opportunities in 2015 was considerable in 2016, full end-to-end cybersecurity testing of the ALIS architecture, from the operational ALOU to the air vehicle, remains to be completed. The JOTT is planning concurrent assessments of the ALIS 2.0.2 Squadron Kit, CPE, and ALOU in 2017. The JOTT is also exploring testing opportunities on the F-35 training systems, and has begun exploring options for testing systems at the U.S. Reprogramming Laboratory, which generates mission data files for the F-35.
- The JPO continued to develop its Operationally Representative Environment (ORE); it plans to perform verification, validation, and accreditation (VV&A) testing in order to conduct future operational testing on ALIS components within the ORE. Regardless of whether the ORE completes VV&A, the JOTT is working with the JPO and Lockheed Martin to plan cybersecurity testing of ALIS components within the ORE for purposes of risk reduction ahead of continued cybersecurity testing of the operational ALIS systems.

DOT&E Response to Senator McCain's Questions Regarding the Completion of SDD

In a letter to the SECDEF on November 3, 2016, Senator McCain asked the Department to respond to questions regarding the completion of SDD. The letter was prompted by, and cited, recent revelations that the program would be experiencing yet another delay in completing SDD and cost overruns that may be upwards of $1 Billion.

Although USD(AT&L) responded to the Senator on behalf of the Department in a letter dated December 19, 2016, the following are DOT&E's responses to each of the questions.

Question #1: When will the Department complete the SDD phase of the F-35?

- DOT&E Answer: SDD will close out in multiple phases. Developmental flight testing is projected to end no earlier than mid-2018, based on independent estimates on completing mission systems flight testing – the testing that will likely take the longest to complete. These estimates—from the Director of Cost Assessment and Program Evaluation (CAPE) of March 2018, the Director of Developmental Test and Evaluation of March to June 2018, Deputy Assistant Secretary of Defense for Systems Engineering of July 2018, and my office of July 2018—are all later than the program's estimate, based on the amount of planned mission systems test points remaining. (These estimates are optimistic because they do not fully account for the corrections and verification testing needed for the more than 270 high-priority deficiencies in Block 3F performance identified by a recent review.) Then, incremental deliveries of the Block 3F

[2] Outsider threats have neither physical access nor account privileges to a network; near-sider threats have physical access to a system, but no account or log-in privileges to a network.

capabilities (i.e., flight envelope, weapons, and avionics) for each variant will likely not be completed until late 2018 due to continued delays and discoveries with F-35B and C flight sciences testing, along with weapons testing. Finally, contract close out actions, including specification compliance and verification and validation, will complete no earlier than late 2019. Completion of all required contracting action for the SDD phase will likely continue for a number of years.

Question #2: How many additional funds, in each upcoming fiscal year budget, will be required to complete F-35 SDD?

- DOT&E Answer: Although DOT&E does not conduct independent cost estimates, CAPE estimated that the program would need an additional $550 Million in FY18 to finish the necessary and planned developmental test points and produce additional software versions to fix and verify the important known and documented deficiencies, then an additional $425 Million in FY19 and $150 Million in FY20 to complete SDD. These estimates add up to an additional $1.125 Billion required to complete SDD. The Program Office estimate is about one-half of the CAPE estimate.

Question #3: What other Service priorities will not receive funding in fiscal year 2018 due to the SDD delay and cost overrun?

- DOT&E Answer: Although the program recently claimed that their estimated SDD overrun can be covered by reallocating existing JSF program funding (other than $100 Million in flight test risk), the SDD cost increase will be much larger than the current program estimate for the reasons described in this report. Therefore, the overrun will not be completely covered with only program funds and the Services will likely need to address the SDD cost increase from within their budgets, or funding currently designated for Follow-on Modernization (FoM) will need to be reallocated to complete SDD.

Question #4: Is Secretary James' Block 3F full combat capability certification, as required by the Fiscal Year 2016 NDAA, still valid?

- DOT&E Answer: For many reasons, it is clear that the Lot 10 aircraft that will begin delivery in early 2018 will not initially have full Block 3F capability. These reasons include, but are not limited to, the following:
  - Envelope limitations will likely restrict the full planned Block 3F carriage and employment envelopes of the AIM-120 missile and bombs well into 2018, if not later.
  - The full set of geographically specific area of responsibility mission data loads (MDLs) will not be complete, i.e., developed, tested and verified, until 2019, at the soonest, due to the program's failure to provide the necessary equipment and software tools for the U.S. Reprogramming Laboratory (USRL).
  - Even after the MDLs are delivered, they will not be tested and optimized to deal with the full set of threats present in IOT&E, let alone in actual combat, which is part of full combat capability.
  - The program currently has more than 270 Block 3F unresolved high-priority (Priority 1 and Priority 2, out of a 4-priority categorization) performance deficiencies, the majority of which cannot be addressed and verified prior to the Lot 10 aircraft deliveries.
  - The program currently has 17 known and acknowledged failures to meet the contract specification requirements, all of which the program is reportedly planning to get relief from the SDD contract due to lack of time and funding.
  - Dozens of contract specification requirements are projected to be open into FY18; these shortfalls in meeting the contract specifications will translate into limitations or reductions to full Block 3F capability.
  - Estimates to complete Block 3F mission systems extend into the summer of 2018, not just from DOT&E, but other independent Department agencies, making delivery of full capability in January 2018 nearly impossible to achieve, unless testing is prematurely terminated, which increases the likelihood the full Block 3F capabilities will not be adequately tested and priority deficiencies fixed.
  - Deficiencies continue to be discovered at a rate of about 20 per month, and many more will undoubtedly be discovered during IOT&E.
  - ALIS version 3.0, which is necessary to provide full combat capability, will not be fielded until mid-2018; also, a number of capabilities that had previously been designated as required for ALIS 3.0 are now being deferred to later versions of ALIS (i.e., after summer of 2018).
  - The Department has chosen to not fund the CAPE estimate for the completion of Block 3F mission systems testing lasting until mid-2018, an estimate which is at least double the Program Office's latest unrealistic estimate to complete SDD. This guarantees the program will attempt a premature resource- and schedule-driven shutdown of mission systems testing, which will increase the risk of mission failures during IOT&E and, more importantly, if the F-35 is used in combat.
  - Finally, rigorous operational testing, which provides the sole means to evaluate actual combat performance, will not complete until at best the end of 2019—and more likely later.

Question #5: How will this delay and cost overrun affect the current overall schedule for Joint Strike Fighter deliveries to the Services?

- DOT&E Answer: The Program Office currently has no plans to delay the production and delivery schedule of aircraft to the Services. However, since Lot 10 aircraft will not initially be delivered with full combat capability, including operational MDLs for Block 3F, the Services will need to plan for accepting aircraft with less capability, possibly with Block 3i capability, until full Block 3F capability can be delivered.

Question #6: When will you complete the operational test and evaluation phase?

- DOT&E Answer: The IOT&E is planned to cover a span of approximately 12 months, and will start after the program is able to meet the TEMP entrance criteria and the Department certifies that the program is ready for test. These entrance criteria are common-sense and carefully defined requirements that were well-coordinated with the Services and JPO as the TEMP was being staffed. Meeting these criteria to enter IOT&E is necessary to ensure the test is conducted efficiently and effectively within the time span planned and to minimize the risk of failing IOT&E, or causing a "pause test" and having to reaccomplish costly test trials, which would only further delay the completion of IOT&E and increase program costs. Since the program will not be ready to start IOT&E until late 2018, at the earliest, and more likely 2019, completion of IOT&E will not occur until late 2019 or early 2020.

Question #7: When will you make the Milestone C/Full-Rate Production decision?

- DOT&E Answer: Since the Milestone C/Full-Rate Production decision cannot be made until after IOT&E is completed and DOT&E has issued its report, it cannot occur by the threshold date of October 2019 and will likely not occur until early 2020, at the soonest.

Question #8: Will you defer any planned F-35 capabilities from SDD into the F-35 Follow-on Modernization (FoM) program?

- DOT&E Answer: Multiple F-35 capabilities will be deferred from SDD or not function properly in Block 3F unless the program continues testing and fixing deficiencies. The program currently has hundreds of unresolved deficiencies and immature capabilities, including 17 documented failures to meet specification requirements for which the program acknowledges and intends to seek contract specification changes in order to close out SDD.

Question #9: How will the SDD delay affect the Follow-on Modernization (FoM) program?

- DOT&E Answer: Delays to the completion of SDD will impact both the FoM program schedule and content. While FoM is critical for the capabilities needed with the F-35 and the program is attempting to minimize delays, the program does not appear to be ready to complete all prerequisites to start full development in FY18, as planned. Also, IOT&E will not be complete until late 2019 or early 2020, which overlaps with the planned test periods for Block 4.1. Finally, the program's current plans for FoM are not executable, for many reasons, which include the following:
  - Too much technical content for the production-schedule-driven developmental timeline
  - Overlapping capability increments without enough time for deficiencies from OT to be fixed prior to releasing the next increment
  - High risk due to excessive technical debt and deficiencies from the balance of SDD and IOT&E being carried forward into FoM because the program does not have a plan or funding to resolve key deficiencies from SDD prior to attempting to add the planned Block 4.1 capabilities
  - Inadequate test infrastructure (aircraft, laboratories, personnel) in the current FoM plan to meet the testing demands of the capabilities planned and the multiple configurations (i.e., TR2, TR3, and Foreign Military Sales)
  - Insufficient time for conducting adequate DT and OT for each increment

Question #10: When will you provide your final response either to validate the current requirement for the F-35 Joint Strike Fighter total program of record quantity or identify a new requirement for the total number of F-35 aircraft that the Department would ultimately procure?

- DOT&E Answer: DOT&E is not aware of when the Department will complete these actions.

Recommendations

- Status of Previous Recommendations. The program adequately addressed 5 of the 14 previous recommendations. As discussed in the appropriate sections of this report, the program did not, and still should:
  1. Acknowledge schedule pressures that make the start of IOT&E in August 2017 unrealistic and adjust the program schedule to reflect the start of IOT&E no earlier than late CY18.
  2. The Department should carefully consider whether committing to a "block buy" is prudent given the state of maturity of the program, as well as whether the block buy is consistent with a "fly before you buy" approach to defense acquisition and the requirements of title 10 U.S. Code.
  3. Plan and program for additional Block 3F software builds and follow-on testing to address deficiencies currently documented from Blocks 2B and 3i, deficiencies discovered during Block 3F developmental testing, and during IOT&E, prior to the first Block 4 software release planned for 2020.
  4. Ensure the testing of Block 3F weapons prior to the start of IOT&E leads to a full characterization of fire-control performance using the fully integrated mission systems capability to engage and kill targets.
  5. Provide the funding and accelerate contract actions to procure and install the full set of upgrades recommended by DOT&E in 2012, correct stimulation problems, and fix all of the tools so the USRL can operate efficiently before Block 3F mission data load development begins.
  6. Complete the planned testing detailed in the DOT&E-approved USRL mission data optimization operational test plan and amendment. Although some

testing was completed, the program should ensure all operational Block 3i MDLs are tested per the approved test plan.

7. Along with the Navy and Marine Corps, conduct an actual operational test of the F-35B onboard an L-class ship before conducting a combat deployment with the F-35B. This test should have the full Air Combat Element (ACE) onboard, include ordnance employment and the full use of mission systems, and should be equipped with the production-representative support equipment.
8. Develop a solution to address the modification and retrofit schedule delays for production-representative operational test aircraft for IOT&E. These aircraft must be similar to, if not from, the Lot 9 production line.
9. Develop an end-to-end ALIS test venue that is production representative of all ALIS components. Although the program has developed the ORE, only limited testing has occurred.

- FY16 Recommendations.

1. The program should complete all necessary Block 3F baseline test points. If the program uses test data from previous testing or added complex test points to sign off some of these test points, the program must ensure the data are applicable and provide sufficient statistical confidence prior to deleting any underlying build-up test points.
2. In light of the fact that the program is unable to correct all open deficiencies prior to IOT&E, the program should assess and mitigate the cumulative effects of the many remaining SDD deficiencies on F-35 effectiveness and suitability, especially those deficiencies that, in combination or alone, may cause operational mission failures during IOT&E or in combat, prior to finalizing and fielding Block 3F. The program will need to add test points to troubleshoot and address deficiencies that are currently not resolved.
3. The program should consider developing another full version of Block 3F software to deliver to flight test in order to address more known deficiencies.
4. The program should ensure adequate resources remain available (personnel, labs, flight test aircraft) through the completion of IOT&E to develop, test, and verify corrections to deficiencies identified during flight testing.
5. The program should address the deficiency of excessive F-35C vertical oscillations during catapult launches within SDD to ensure catapult operations can be conducted safely during IOT&E and during operational carrier deployments.
6. The Program Office must immediately fund and expedite the contracting actions for the necessary hardware and software modifications to provide the necessary and adequate Block 3F mission data development capabilities for the USRL, including an adequate number of additional radio frequency signal generator channels and the other required hardware and software tools.
7. The program should address the JOTT-identified shortfalls in the USRL that prevent the lab from reacting to new threats and reprogramming mission data files consistent with the standards routinely achieved on legacy aircraft.
8. The program should correct deficiencies that are preventing completion of all of the TEMP-required Block 3F Weapons Delivery Accuracy (WDA) events and ensure the events are completed prior to finishing SDD.
9. The program should ensure Block 3F is delivered with capability to engage moving targets, such as that provided by the GBU-49, or other bombs that do not require lead-laser guidance.
10. The program should complete additional testing and analysis needed to determine the risk of pilots being harmed by the Transparency Removal System (which shatters the canopy first, allowing the seat and pilot to leave the aircraft) during ejections in other than ideal, stable conditions (such as after battle damage or during out-of-control situations). The program should complete these tests as soon as possible, with the new equipment, including the Gen III Lite helmet in a variety of off-nominal conditions, so that the Services can better assess risk associated with ejections under these "off-nominal" conditions.
11. The program needs to conduct an assessment to determine the extent to which the results of further durability testing with BH-1, the F-35B durability test article, are representative of production aircraft and, if necessary, procure another test article for the third life testing.
12. The Navy and the Program Office should investigate alternatives for determining the operational impact of an engine removal and install while conducting carrier air wing operations at sea.
13. The Navy and Marine Corps should conduct an analysis, such as an operational logistics footprint study, which simulates flight deck and hangar bay spotting (aircraft placement) with a full ACE onboard, using data from the DT-III ship trials to determine what the impact of an engine removal and installation would be on integrated ship and ACE operations with a full ACE onboard.
14. The program and the Navy should investigate if the heavy power module container should be redesigned for better usability at sea.
15. The program and the Navy should investigate potential options to improve ship-based communications bandwidth dedicated to ALIS connectivity off-ship, such as increasing the priority of ALIS transmissions, or reserving low-use times of the day for handling large volumes of ALIS message traffic.
16. The Navy should investigate any efficient, multi-use opportunities for F-35 support equipment (SE) such as using legacy SE on the F-35 or F-35 SE on legacy aircraft.
17. The Navy should investigate options for increasing the number of wall power outlets in CVN hangar bays to help facilitate simultaneous maintenance on multiple F-35Cs, or the ability to interconnect multiple pieces of support equipment from a single outlet to permit simultaneous operations.

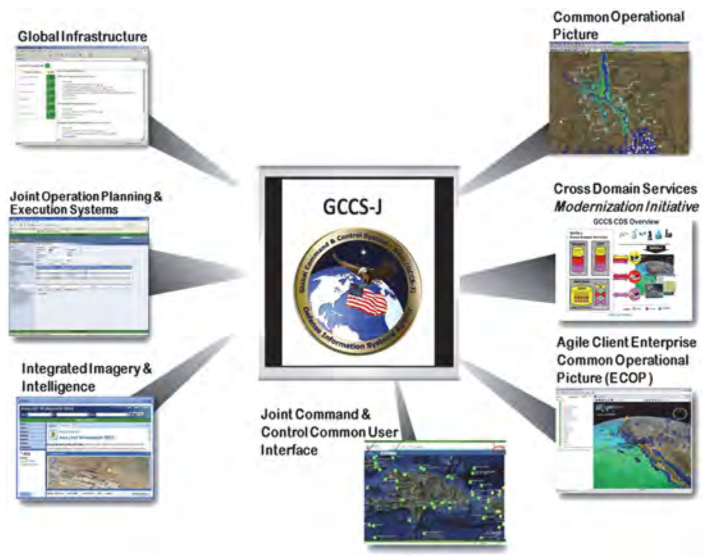
Global Command and Control System – Joint (GCCS-J)

Executive Summary

- In FY16, the Defense Information Systems Agency's (DISA) development of Global Command and Control System – Joint (GCCS-J) focused on three elements of the system: Global v6.0, Agile Client Release 7 v5.1.0.1, and Joint Operation Planning and Execution System (JOPES) v4.2.0.4.
  - Global v6.0 and Agile Client Release 7 v5.1.0.1 represent the first phase of development to replace the full capabilities of the currently fielded Global v4.3 Update 1 Emergency Release 1.
  - JOPES v4.2.0.4 supports migration to 64-bit applications, Public Key Infrastructure implementation on web servers, and security enhancements.

Global

- The Joint Interoperability Test Command (JITC) conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) on Global v4.3 Update 1 Emergency Release 1 at U.S. Pacific Command (USPACOM), Camp H.M. Smith, Hawaii, from December 2015 through January 2016. During this CVPA and AA, JITC verified and assisted in the correction and mitigation of vulnerabilities discovered during previous assessments and improved the system's cybersecurity posture as deployed at USPACOM Headquarters. However, GCCS-J remains vulnerable to cyber exploitation by an adversary with limited-to-moderate cyber capabilities.
- JITC conducted the Global v6.0 and Agile Client Release 7 v5.1.0.1 operational assessment (OA) at U.S. Central Command, MacDill AFB, Florida, and U.S. Strategic Command, Offutt AFB, Nebraska, from August 2 – 9, 2016.
- JITC evaluated 18 of 22 capability areas delivered in this initial Global v6.0 and Agile Client Release 7 v5.1.0.1. Users successfully completed the majority of mission tasks in all delivered capability areas. However, users identified significant defects in six capability areas.
- Global v6.0 and Agile Client Release 7 v5.1.0.1 are not suitable for all users. More than half of Global users (6 of 11) believe these systems cannot support real-world combat operations due to performance problems and capability gaps. The remaining users indicated that the systems need updates to be suitable.
- JITC will conduct an AA, once the program manager fields Global v6.0 and Agile Client Release 7 v5.1.0.1.
- DOT&E will evaluate Global v6.0 and Agile Client Release 7 v5.1.0.1 effectiveness and suitability, once the program manager delivers a more complete set of capabilities. The OA was adequate to evaluate initial system capabilities.



JOPES

- JITC conducted the JOPES v4.2.0.4 operational test from September 28 through October 14, 2016.
- JOPES v4.2.0.4 is operationally effective for all Services except the Air Force. JOPES v4.2.0.4 users successfully created operational plans and force requirements; sourced, updated, and validated force requirements; and completed scheduling and movement of forces. Air Force Deliberate and Crisis Action Planning and Execution Segments (DCAPES) users were unable to source Combatant Command force requirements due to a JOPES v4.2.0.4 to DCAPES interface defect. All other Service Force Providers and JOPES users were able to successfully source force requirements.
- JOPES v4.2.0.4 is operationally suitable. Users found JOPES v4.2.0.4 performance and usability comparable to the currently fielded version. JOPES v4.2.0.4 met the availability threshold of 99.7 percent.
- JOPES v4.2.0.4 survivability is undetermined. JITC initiated the JOPES v4.2.0.4 CVPA in April 2015, but the discovery of system defects prevented completion. JITC plans to complete the CVPA and conduct an AA on the fielded version of JOPES v4.2.0.4.

System

- GCCS-J consists of hardware, software (both commercial off-the-shelf and government off-the-shelf), procedures, standards, and interfaces that provide an integrated, near real-time picture of the battlespace that is necessary to conduct joint and multi-national operations. Its client/server architecture uses open systems standards and government-developed military planning software. Global and JOPES are two of the baseline systems that comprise the operational environment of GCCS-J.

Global (Force Protection, Situational Awareness, and Intelligence applications)

- Global v4.3 Update 1 Emergency Release 1 is the currently fielded version. DISA developed Global v4.3 Update 1 to implement high-priority intelligence mission updates to the Theater Ballistic Missile correlation systems, Joint Targeting Toolbox, and Modernized Integrated Database. Emergency Release 1 resolved an operational deficiency discovered in the fielded Global v4.3 Update 1 software and included some of the improvements originally planned for the canceled Global v5.0.
- Global v6.0 and Agile Client Release 7 v5.1.0.1 represent the first phase of a development plan to replace the full capabilities of Global v4.3 Update 1 Emergency Release 1. Global v6.0 will provide back-end services, databases, and system administration functions. Agile Client Release 7 v5.1.0.1 (Agile Client core services and the Agile Client plug-in) provides visualization and presentation of GCCS-J mission applications and functionality to the user.

JOPES (Force Employment, Projection, Planning, and Deployment/Redeployment applications)

- JOPES v4.2.0.3 Emergency Release 4 is the currently fielded version. DISA developed JOPES v4.2.0.3 Emergency Release 4 to implement Global Force Management capabilities. This release added Force Tracking Number and Deployment Order information to the system, as well as an ability to identify and query operationally relevant plans. DISA also corrected seven critical deficiencies.
- JOPES v4.2.0.4 supports migration to 64-bit applications, Public Key Infrastructure implementation on web servers, security enhancements, and resolves 25 problem reports. While this release does not introduce new user capabilities, the changes affect all critical mission areas and external interfaces.

Mission

- Joint Commanders utilize the GCCS-J to accomplish command and control.

Global

- Commanders use Global to:
  - Link the National Command Authority to the Joint Task Force, Component Commanders, and Service-unique systems at lower levels of command
  - Process, correlate, and display geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture
  - Provide Integrated Imagery and Intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture and allow commanders to manage and produce target data using the Joint Tactical Terminal
  - Provide a missile warning and tracking capability
- Air Operations Centers use Global to:
  - Build the air picture portion of the common operational picture and maintain its accuracy
  - Correlate or merge raw track data from multiple sources
  - Associate raw Electronics Intelligence data with track data
  - Perform targeting operations

JOPES

- Commanders use JOPES to:
  - Translate policy decisions into operations plans that meet U.S. requirements to employ military forces
  - Support force deployment, redeployment, retrograde, and re-posturing
  - Conduct contingency and crisis action planning

Major Contractors

- Government Integrator: DISA
- Software Developers:
  - Northrop Grumman – Arlington, Virginia
  - Leidos – Arlington, Virginia
  - Pragmatics – Arlington, Virginia

Activity

Global

- JITC conducted a CVPA and AA on GCCS-J v4.3 Update 1 Emergency Release 1 at USPACOM, Camp H.M. Smith, Hawaii, from December 2015 through January 2016.
- JITC conducted the Global v6.0 and Agile Client Release 7 v5.1.0.1 OA at U.S. Central Command, MacDill AFB, Florida, and U.S. Strategic Command, Offutt AFB, Nebraska, from August 2 – 9, 2016, in accordance with a DOT&E-approved policy that did not require a DOT&E-approved test plan.

JOPES

- JITC conducted the JOPES v4.2.0.4 operational test from September 28 through October 14, 2016, in accordance with a DOT&E-approved policy that did not require a DOT&E-approved test plan. U.S. Africa Command, Kelly Barracks, Germany; U.S. European Command, Patch Barracks, Germany; USPACOM, Camp H.M. Smith, Hawaii; Combatant Command components; and Force Providers participated in the operational test.

Assessment

Global

- During the Global v4.3 Update 1 Emergency Release 1 CVPA and AA, JITC verified and assisted in the correction and mitigation of vulnerabilities discovered during previous assessments and improved the system's cybersecurity posture as deployed at USPACOM Headquarters. However, GCCS-J remains vulnerable to cyber exploitation by an adversary with limited-to-moderate cyber capabilities.
- JITC evaluated 18 of 22 capability areas delivered in this initial Global v6.0 and Agile Client Release 7 v5.1.0.1. Users successfully completed the majority of mission tasks in all delivered capability areas. However, users identified significant defects affecting six capability areas:
  - Manage Common Operational Picture. Poor Agile Client Release 7 v5.1.0.1 performance under an operationally realistic track load restricts Combatant Command situational awareness. Users experienced Agile Client Release 7 v5.1.0.1 freezes, requiring a manual restart, under an operationally realistic track load (55,000 tracks). To complete testing, users applied database filters on the Global v6.0 server to limit tracks sent to Agile Client (less than 10,000 tracks). With filters applied, Agile Client performance was acceptable, and users successfully completed mission tasks.
  - Manage Track Data. Users lost previously created bookmarks, plug-in downloads, and filter templates due to Agile Client Release 7 v5.1.0.1 freezes and experienced excessive downtime regaining access or recreating them.
  - Manage Intelligence Data. Users could not associate an image to a joint desired point of impact target in Global v6.0, which could lead to an analyst associating the wrong image or coordinates for a mission folder.
  - Support Battle Damage Assessment. Users were unable to delete associations between targets and target records in Global v6.0. To maintain target record accuracy, users regularly refine intelligence data and break associations with out of date records.
  - Support Missile Defense. Users were unable to view raw data reports for missile tracks because Global v6.0 does not interface with the Integrated Broadcast System. Global v6.0 currently receives missile reports using the Common Operational Picture Synchronization Tools interface. Users rely on these reports in the currently fielded Global v4.3 Update 1.
  - Reconstruct Historical Events. The Agile Client Release 7 v5.1.0.1 does not have the ability to record missile events as they occur or replay them as needed. Users rely on this capability in the currently fielded Global v4.3 Update 1.
- Global v6.0 and Agile Client Release 7 v5.1.0.1 are not suitable for all users. More than half of Global users (6 of 11) believe the systems cannot support real-world combat operations due to performance problems and capability gaps. The remaining users indicated that the systems need updates to be suitable.
- Users felt Global v6.0 and Release 7 v5.1.0.1 online training did not provide necessary knowledge to conduct mission tasks.
- JITC will conduct an AA once the program manager fields Global v6.0 and Agile Client Release 7 v5.1.0.1.
- DOT&E will evaluate Global v6.0 and Agile Client Release 7 v5.1.0.1 effectiveness and suitability once the program manager delivers a more complete set of capabilities. The OA was adequate to evaluate initial system capabilities.

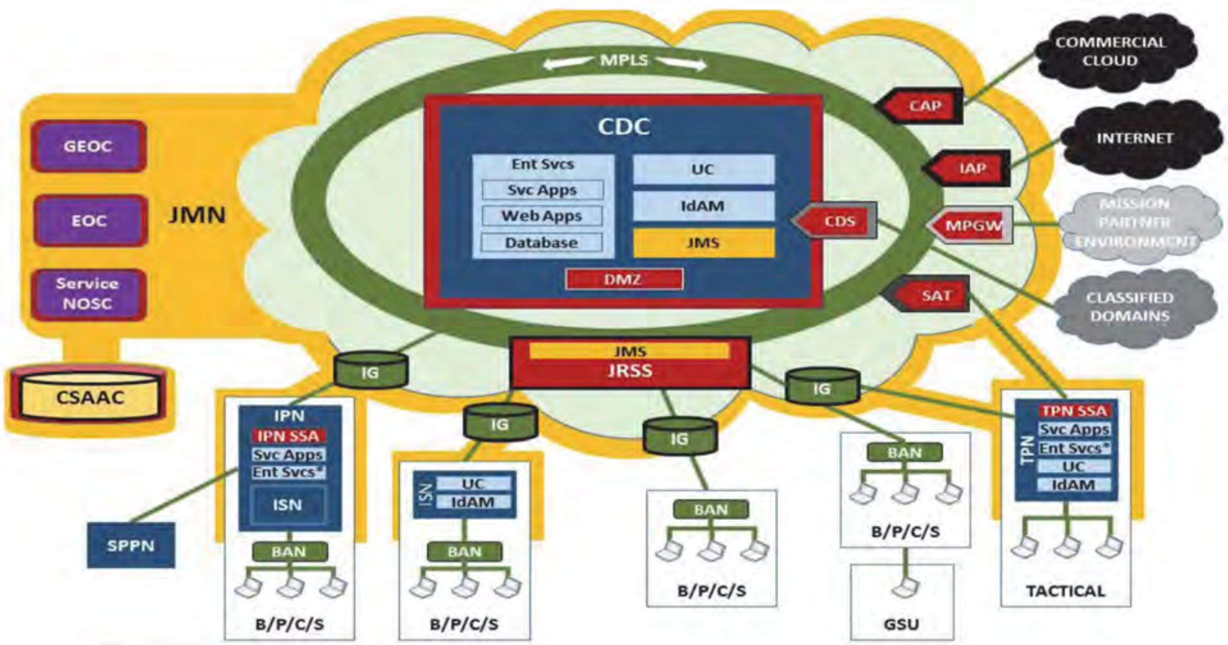
JOPES

- JOPES v4.2.0.4 is operationally effective for all Services except the Air Force. JOPES v4.2.0.4 users successfully created operational plans and force requirements; sourced, updated, and validated force requirements; and completed scheduling and movement of forces. Air Force DCAPES users were unable to source Combatant Command force requirements due to a JOPES v4.2.0.4 to DCAPES interface defect. The interface defect significantly affects the Air Force, which relies on DCAPES for sourcing force requirements. All other Service Force Providers and JOPES users were able to successfully source force requirements.
- JOPES v4.2.0.4 is operationally suitable. Users found JOPES v4.2.0.4 performance and usability comparable to the currently fielded version. JOPES v4.2.0.4 met the availability threshold of 99.7 percent. System administrators successfully installed and configured the system using the available documentation.
- JOPES v4.2.0.4 survivability is undetermined. JITC initiated the JOPES v4.2.0.4 CVPA in April 2015, but the discovery of system defects prevented completion. JITC plans to complete the CVPA and conduct an AA on the fielded version of JOPES v4.2.0.4.

Recommendations

- Status of Previous Recommendations. DISA has addressed one of the two previous FY15 recommendations. However, DISA still needs to conduct cybersecurity testing of JOPES v4.2.0.3 Emergency Release 4 (or later) in an operational environment to assess protect, detect, react, and restore capabilities.
- FY16 Recommendations. DISA should:
  1. Develop and field mitigations for the discovered vulnerabilities to all Global v4.3 Update 1 Emergency Release 1 locations and verify that the vulnerabilities have been corrected.
  2. Correct Global v6.0 and Agile Client Release 7 v5.1.0.1 deficiencies discovered during the OA.
  3. Correct the DCAPES interface defect and conduct regression testing prior to fielding JOPES v4.2.0.4.
  4. Conduct an AA on the fielded versions of Global v6.0 and Agile Client Release 7 v5.1.0.1.
  5. Complete the CVPA and conduct an AA on the fielded version of JOPES v4.2.0.2.

Joint Information Environment (JIE)



B/P/C/S - Base, Post, Camp, and Station
BAN - Base Area Network
CAP - Cloud Access Point
CDC - Core Data Center
CDS - Cross Domain Solution
CSAAC - Cyber Situational Awareness Analytic Cloud
Data Svcs - Data Services
DMZ - Demilitarized Zone
Ent Svcs - DOD Enterprise Services (*Extended)
EOC - Enterprise Operations Center
GEOC - Global Enterprise Operations Center
GSU - Geographic Separated Unit
IAP - Internet Access Point
IdAM - Identitiy and Access Managment
IG - Installation Gateway
IPN - Installation Processing Nodes
ISN - Installation Service Node
JMN - JIE Management Network
JMS - JIE Management System
JRSS - Joint Regional Security Stacks
MPGW - Mission Partner Gateway
MPLS - Multiprotocol Label Switching
NOSC - Network Operations & Security Center
SAT - Satellite Communications Gateway
SPPN - Special Purpose Processing Node
SSA - Single Security Architecture
Svc Apps - DOD Component Applications
TPN - Tactical Processing Node
UC - Unified Capabilities
Web Apps - Web Applications

Executive Summary

- Although the Joint Information Environment (JIE) is not a program of record, numerous programs, including but not limited to the Joint Regional Security Stack (JRSS), are directly associated with JIE, are expending significant and substantial resources, and are meant to execute critical missions. To date, the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), and Services have not conducted rigorous and comprehensive operational testing of any of the programs associated with JIE.
- The JIE Test and Evaluation Working Group, supported by DOT&E, the DOD Chief Information Officer (CIO), U.S. Cyber Command, and the Joint Staff J6 is developing a JIE test and evaluation strategy to assess the maturity of JIE capabilities through a series of annual operational assessments and an overarching operational test and evaluation, starting in July 2017.
- JIE efforts continue to lack an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors.
- DISA and the Services are pursuing a non-traditional acquisition approach for the JRSS that has led to early Army and Air Force fielding decisions uninformed by rigorous and comprehensive operational tests, despite the results of developmental tests and limited-in-scope operational assessments indicating JRSS users are not able to provide effective network security. Given the preeminent role that JRSS, once fielded, necessarily plays in securing the Department's networks, this early fielding of JRSS under circumstances in which users seem unable to employ it to secure their networks may unnecessarily jeopardize the security of critical DOD networks and systems.
- DOT&E and JITC planned for an operational assessment in December 2016 on the JRSSs fielded by the Air Force, but in late November 2016 the Air Force elected to postpone the assessment because of known problems with JRSS technology, training, and enterprise management and operator procedures, which severely limit the current cybersecurity effectiveness of the already fielded JRSS installations. Specifically, the 24th Air Force Commander was concerned that DOT&E might issue a report that reflected poorly on JRSS.
- In response to the DOT&E memos on JIE/JRSS signed in August and September 2016, the DOD CIO agreed that an

IOT&E event for JRSS will take place in May 2017, but this date will likely be revised based on the Air Force deferral of testing.

Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE as a secure environment, comprised of shared information technology (IT) infrastructure, enterprise services, and single security architecture.
- JIE consists of multiple subordinate programs, projects, and initiatives managed by DISA and the Services.
- The DOD CIO has prioritized areas of modernization of the DOD Information Network (DODIN) for DOD components to implement as the foundation for JIE. The DOD CIO's areas of modernization include the following:
  - Optical carrier upgrades and Multi-Protocol Label Switching (MPLS)
  - JRSS, the Joint Management System for JRSS, and Cyber Situational Awareness Capabilities
  - The Computing Environment, which includes Commercial Cloud, Cloud Access Points, and milCloud
  - The Mission Partner Environment-Information System, for coalition/partner information sharing, and the Mission Partner Gateways
  - Mobility for unclassified and classified capabilities
- The JCS envision JIE as a shared information technology construct for DOD to reduce costs, improve and standardize physical infrastructure, increase the use of enterprise services, improve IT effectiveness, and centralize the management of network security. The Joint Staff specifies the following enabling characteristics for JIE capability:
  - Transition to centralized data storage
  - Rapid delivery of integrated enterprise services (such as email and collaboration)
  - Real-time cybersecurity awareness
  - Scalability and flexibility to provide new services
  - Use of common standards and operational techniques
  - Transition to a single security architecture
- The DOD CIO, DISA, and Services plan to achieve the JIE goals via the following interrelated initiatives:
  - Consolidate applications and data into the cloud or into centralized regional or global data centers that are not segregated by military Service.
  - Establish enterprise operation centers to centralize network management and defense.
  - Upgrade the network infrastructure to include MPLS routers and optical transport upgrades, which enhances network resiliency and bandwidth capacity, and improves security.
  - Implement JRSS architecture and other security constructs as part of a single security architecture. This will reduce the number of access points to the DODIN, standardize identity and access management, and enable centralized defensive cyber operations.
- JIE is not a program of record and does not have a traditional milestone decision authority, program executive organization, and project management structure that would normally be responsible for the cost, schedule, and performance of a program. Moreover, an Operational Test Agency has not conducted independent operational testing required of a traditional acquisition program of record.
- The DOD CIO generally leads JIE efforts with support from the JIE Executive Committee (EXCOM) – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6 – which provides JIE direction, objectives, and limited accountability. DISA is the principal integrator for JIE services and testing.

Activity

- DISA and the Services continued implementation of key JIE enabling capabilities in the United States and in the European theater with the establishment of additional JRSS and MPLS capabilities.
  - JITC conducted an assessment of the JRSS version 1.0 with a Red Team to evaluate Army JRSS operations in December 2015 and published a test report in April 2016.
  - JITC conducted lab-based JRSS developmental testing and operational rehearsals during 2016.
  - In August 2016, the Air Force conducted an evaluation of JRSS with the objective of informing an Air Force JRSS operational trial period entry decision in September 2016. The Air Force decided to migrate three sites behind JRSS for operational trials, starting in October 2016, with plans to accelerate migration efforts in January 2017.
- The General Accountability Office published its JIE report in July 2016.
- In August and September 2016, DOT&E published three JIE/JRSS memos to the Services recommending that they conduct operational testing to ensure that the fielding decision authorities have full understanding of the capabilities and limitations that JRSS will provide before deciding to migrate to JRSS and depend upon it to protect their networks.
- DOT&E and JITC planned for an operational assessment in December 2016 on the JRSSs fielded by the Air Force, but in late November 2016 the Air Force elected to postpone the assessment because of known problems with JRSS technology, training, and enterprise management and operator procedures, which severely limit the current cybersecurity effectiveness of the already fielded JRSS installations. Specifically, the 24th Air Force Commander was concerned that DOT&E might issue a report that reflected poorly on JRSS.
- In response to the DOT&E memos on JIE/JRSS signed in August and September 2016, the DOD CIO issued a memo

in September 2016 agreeing that an IOT&E event for JRSS will take place in May 2017, but this date will likely be revised based on the Air Force deferral of testing. The DOD CIO memo also said that final JRSS migrations will not occur until operational testing satisfies the Military Services' requirements.
- The IOT&E event planned for May 2017 will inform Air Force leadership decisions to fully decommission legacy capabilities. Until full decommissioning occurs, it would be relatively easy to switch from JRSS back to legacy capabilities, if the Air Force chose to do so.
- The JIE Test and Evaluation Working Group, supported by DOT&E, the DOD CIO, U.S. Cyber Command, and the Joint Staff J6 is developing a JIE test and evaluation strategy.
- In August 2016, U.S. Cyber Command initiated an effort to develop a strategic direction for leveraging JRSS capabilities in support of their secure, operate, and defend the DODIN mission.

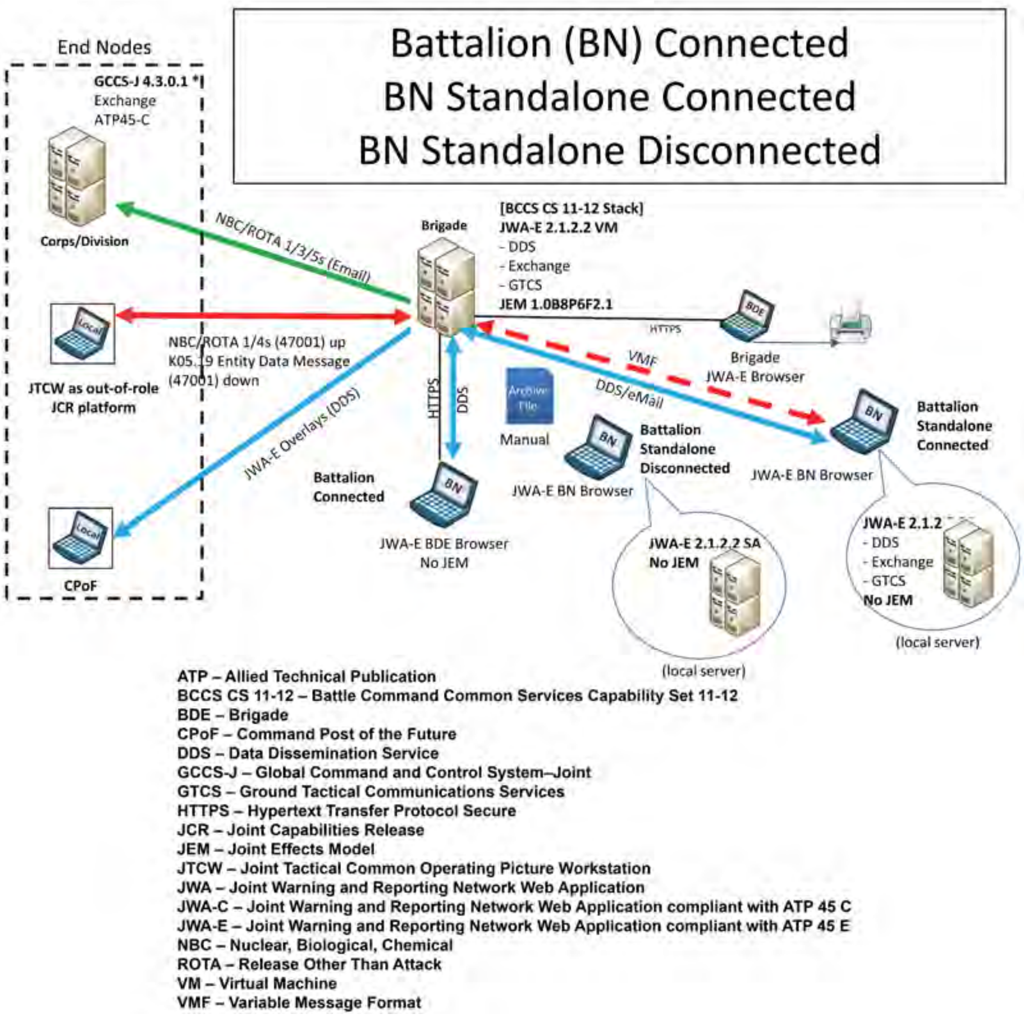
Assessment
- Although JIE is not a program of record, numerous programs, including but not limited to JRSS, are directly associated with JIE, are expending significant and substantial resources, and are meant to execute critical missions. To date, DISA, JITC, and the Services have not conducted rigorous and comprehensive operational testing of any of the programs associated with JIE.
- DISA and the Services are pursuing a non-traditional acquisition approach for the JRSS that has led to early Army and Air Force fielding decisions uninformed by rigorous and comprehensive operational tests, despite the results of developmental tests and limited-in-scope operational assessments indicating JRSS users are not able to provide effective network security. Given the preeminent role that JRSS, once fielded, necessarily plays in securing the Department's networks, this early fielding of JRSS under circumstances in which users seem unable to employ it to secure their networks may unnecessarily jeopardize the security of critical DOD networks and systems.
- Acquiring and deploying JRSS without operational testing significantly increases risks to the missions and forces which rely on the affected networks. The limited early test data reported by JITC in April 2016 shows that JRSS capabilities are immature, lacking a stable configuration, and that operator training is incomplete and insufficient. Of most concern is JITC's finding that key JRSS cybersecurity functions are not mission capable.
- Testers identified over three dozen deficiencies, including many scored as Category 1 Emergency and Category 1 Urgent priority problems.
  - Substandard JRSS capability performance areas included system scalability; reliable connectivity to JRSS components over the network; the absence of standardized tactics, techniques, and procedures; and inadequate operator proficiency, training, and documentation.
  - These problems affected critical capabilities and adversely affect the operational effectiveness of defensive cybersecurity operations.
  - Network traffic during the test traversed in series on both the JRSS and the existing Air Force gateway security stacks, with each stack potentially interfering with and affecting the function of the other security stack.
- Despite these test results, the Air Force plans to start fielding the JRSS to 14 bases between October and December 2016; the Army and Navy are also fielding, but at a slower pace.
- Fielding JRSS prior to verifying through rigorous operational testing and regressions that the technology works, and that JRSS operators and enterprise network defenders have effective procedures and training required to operate the system, risks degrading DOD network operations and security, potentially leaving networks vulnerable to undetected adversarial actions during and after JRSS migration.
- The DOD CIO is the lead for JIE governance; however, the JIE effort continues to lack an overarching systems integration process or program executive organization to manage cost, drive schedule, and monitor performance factors.

Recommendations
- Status of Previous Recommendations. The DOD CIO and Director of DISA have not addressed the previous FY14 and FY15 recommendations to:
  1. Develop adequate test schedules and plans for anticipated future test events in FY17 and beyond.
  2. Establish an overarching JIE program executive to integrate the system efforts and oversee cost, schedule, and performance.
  3. Manage all key JIE capabilities/components with empowered, responsible program managers.
  4. Continue to develop an overarching test strategy that encompasses not only the upcoming testing of JIE, but also defines the key issues and concepts to be tested in subsequent tests and assessments.
- FY16 Recommendations.
  1. To prevent unnecessary risks to DOD networks, the Services should stop fielding JRSS capabilities until the results of a comprehensive IOT&E show that the enterprise and Service operators are capable of using the JRSS to provide effective network security.
  2. Poor program governance and acquisition oversight for JRSS is jeopardizing the security of DOD networks; to address these issues Congress should consider directing the DOD to make JRSS an Acquisition Category IAM program of record.

  The DOD CIO, JIE EXCOM, and DISA should:

  3. Complete, adopt, and implement the JIE test and evaluation strategy.
  4. Conduct a JRSS IOT&E to evaluate JRSS capabilities, operator training, and enterprise processes and use the results to inform JRSS capability-related fielding and migration decisions.

Joint Warning and Reporting Network (JWARN)



Executive Summary

- The U.S. Army Operational Test Command (OTC) conducted an operational test of the Joint Warning and Reporting Network (JWARN) Web Application E (JWA-E) during an Armored Brigade Combat Team field training exercise from June 9 – 16, 2016, at Fort Hood, Texas.
- JWA-E software is backward compatible and interoperable with JWARN Increment 1 software.
- In a degraded communications environment, JWA-E operating on stand-alone computers provides battalion chemical, biological, radiological, and nuclear (CBRN) operators an automated capability to create, edit, and correlate CBRN reports to support battalion leadership.
- Operators of JWA-E on stand-alone Command Post of the Future (CPOF) computers could not see CBRN hazard plots and unit locations on an operational map at the same time to identify units at risk to send CBRN warning reports when not connected to the Brigade Command and Control System (BCCS) servers.

System

- JWARN is a joint automated CBRN warning, reporting, and analysis software tool. It resides on joint and Service command and control systems including the Global Command and Control System (GCCS) – Army, GCCS – Joint, GCCS – Maritime, Command and Control Personal Computer/ Joint Tactical Common Workstation, the Army's BCCS server, and on stand-alone computers.
- JWARN software automates the NATO CBRN warning and reporting process to increase the speed and accuracy of information.
- The JWARN Increment 2 program will consist of four phases named after the Requirements Definition Package (RDP) that

identifies the capabilities to be delivered. Each RDP will have multiple software capability drops.

- RDP-1 will update the JWARN Web Application code to comply with recent changes to the NATO Allied Technical Publication 45 and add planning tools previously included in Increment 1 versions of JWARN
- RDP-2 is envisioned to integrate RDP-1 capabilities into the Service command and control system/architectures
- RDP-3 is envisioned to provide capability to integrate with networked sensors
- RDP-4 is anticipated to support modernization and emerging capabilities

Mission

A unit equipped with JWARN provides analysis of potential or actual CBRN hazard areas based on operational scenarios or sensor and observer reports, identifies affected units and operating areas, and transmits warning reports to support commanders' force protection and operational decisions.

Major Contractor

Northrop Grumman Mission Systems – Orlando, Florida

Activity

- In FY16, the Joint Program Office for Information Systems (JPM-IS) delivered the first two capability drops for JWARN Increment 2 RDP 1 referred to as JWA-E. JWA-E operates as a Web Application on the Army's BCCS server and stand-alone CPOF computers. The software is compliant with the NATO Allied Technical Publication – 45 version E.
- JPM-IS conducted developmental testing on JWA-E, at its integration laboratory in San Diego, California, from October 2015 to April 2016.
- JPM-IS and the Army Test and Evaluation Command conducted integrated testing of JWA-E from April 25 – 28, 2016.
- The Army Research Laboratory Survivability/Lethality Directorate conducted a Cooperative Vulnerability and Penetration Assessment of the JWA-E from February 1 – 5, 2016, at Aberdeen Proving Ground, Maryland.
- OTC conducted the JWARN Increment 2 Initial Operational Test – Army 1 (IOT-A1) of the first capability drop during an Armored Brigade Combat Team field training exercise from June 9 – 16, 2016, at Fort Hood, Texas.
- During IOT-A1, OTC conducted an excursion to demonstrate JWARN Increment 2 joint interoperability and backward compatibility by exchanging JWARN messages using a JWA-E operating on a battalion-level CPOF computer in Fort Hood, with the GCCS – Maritime-hosted JWARN Increment 1 operated by Navy personnel in southern California.
- OTC was unable to execute IOT-A1 in accordance with the DOT&E-approved test plan due to network configuration problems and lack of an operational GCCS – Army hosted JWARN Increment 1 system.
- The Army Threat Systems Management Office conducted a cybersecurity Adversarial Assessment during the IOT-A1 that focused on portraying the insider, near-sider, and outsider threats.

Assessment

- JWA-E software is backward compatible and interoperable with JWARN Increment 1 software.
- In a degraded communications environment, JWA-E on stand-alone CPOF computers provides battalion CBRN operators an automated capability to create, edit, and correlate CBRN reports to support battalion leadership.
- When not connected to the BCCS server, operators of the JWA-E on CPOF computers could not see CBRN hazard plots and unit locations on an operational map at the same time to identify units at risk to send CBRN warning reports.
- JWA-E planning tools provide CBRN operators with the capability to generate basic hazard prediction plots to support the development of courses of action in the event of a CBRN incident.
- The JWA-E has cybersecurity vulnerabilities that need to be corrected prior to fielding.

Recommendations

- Status of Previous Recommendations. The JWARN Program Office and the Navy addressed all FY15 recommendations.
- FY16 Recommendations. The JPM-IS should:
    1. Work with the appropriate Army Program Offices to identify a solution so that operators using JWA-E stand-alone can see CBRN hazard plots in relation to operational unit locations to enable timely identification and warning of units at risk.
    2. Correct the cybersecurity vulnerabilities discovered during IOT-A1 prior to fielding.

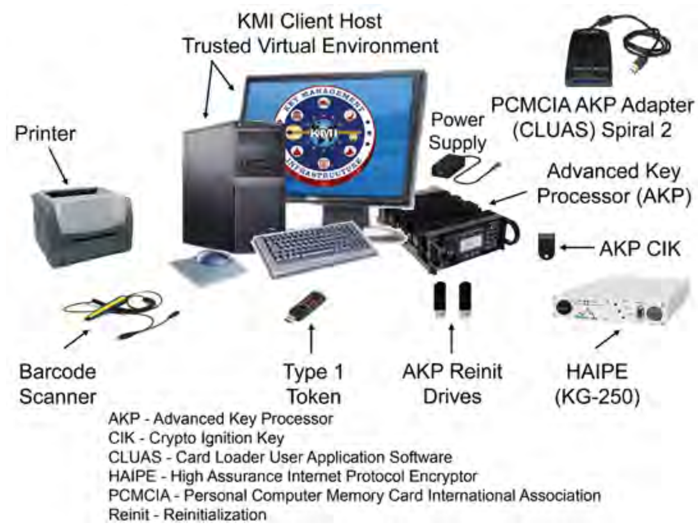
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- DOT&E published its Key Management Infrastructure (KMI) Spiral 2, Spin 1 Limited User Test (LUT) and LUT Retest Report in late October 2015 that found KMI to be operationally effective with some problems and not operationally suitable. The Joint Interoperability Test Command (JITC) conducted a LUT of KMI Spiral 2, Spin 1 capabilities; however, JITC could not fully assess KMI cybersecurity until an Adversarial Assessment is completed in Spin 2.
- Based on the LUT Retest results, USD(AT&L) authorized a limited DOD-wide KMI Spiral 2, Spin 1 fielding in December 2015 with guidance to the National Security Agency (NSA) and the Services to implement mitigation plans to resolve suitability problems discovered during the LUTs.
- Users are satisfied with Spiral 2, Spin 1 capabilities, performance, and system stability. Database management problems during the LUT and LUT Retest affected software downloading. Site failover, Advanced Extremely High Frequency keying, Card Loader, F-22, KMI tokens, benign fill (a cryptographic key wrapped within an encryption key known only between the device wrapping it and the end unit), and existing Spiral 1 functions worked. During the LUT Retest, some problems remained with Mobile User Objective System (MUOS), Secure Software Provisioning, and the Host-Based Security System (HBSS) and its supporting servers.
- In February 2016, the KMI Program Management Office (PMO) changed the Full Deployment Decision (FDD) estimate from April 2017 to February 2018, thus triggering a Significant Change.
- The KMI PMO and JITC conducted a government-led Developmental Test and Evaluation-2 (DT&E-2) of Spiral 2, Spin 2 capabilities in July 2016. Major problems with Spin 2 capabilities required the KMI PMO to delay the DT&E-2 regression event from August to October 2016.
- JITC conducted no KMI operational testing in FY16 due to Spin 2 schedule delays.

System

- KMI will replace the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., encryption keys, cryptographic applications, and account management).
- KMI consists of core nodes that provide web operations at sites operated by the NSA, as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies.



- KMI combines substantial custom software and hardware development with commercial off-the-shelf computer components. The custom hardware includes an Advanced Key Processor for autonomous cryptographic key generation and a Type 1 user token for role-based user authentication. The commercial off-the-shelf components include a client host computer with monitor and peripherals, High Assurance Internet Protocol Encryptor (KG-250), printer, and barcode scanner.

Mission

- Combatant Commands, Services, DOD agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DOD Information Networks, and initiatives such as Cryptographic Modernization.
- Service members will use KMI cryptographic products and services to enable security services (confidentiality, non-repudiation, authentication, and source authentication) for diverse systems such as Identification Friend or Foe, GPS, Advanced Extremely High Frequency Satellite System, and Warfighter Information Network – Tactical.

Major Contractors

- Leidos – Columbia, Maryland (Spiral 2 Prime)
- General Dynamics Information Assurance Division – Needham, Massachusetts (Spiral 1 Prime)
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted a LUT in April 2015 of Spiral 2, Spin 1 capabilities in accordance with a DOT&E-approved test plan, and a LUT Retest in July 2015 to verify fixes to problems discovered during the LUT. JITC published its LUT Retest Report in October 2015. The LUT examined new KMI capabilities for supporting F-22 Raptor, Advanced Extremely High Frequency and MUOS satellite systems, benign fill (a cryptographic key wrapped within an encryption key known only between the device wrapping it and the end unit), Secure Terminal Equipment enhanced cryptographic cards, new KMI tokens, HBSS and ePolicy Orchestrator server, site failover, and EKMS and KMI client workstation transition procedures.
- DOT&E published its KMI Spiral 2, Spin 1 LUT and LUT Retest Report in late October 2015 that found KMI to be operationally effective with some problems and not operationally suitable. JITC conducted a LUT of KMI Spiral 2, Spin 1 capabilities; however, JITC could not fully assess KMI cybersecurity until an Adversarial Assessment is completed in Spin 2.
- Based on the LUT Retest results, USD(AT&L) authorized a limited DOD-wide KMI Spiral 2, Spin 1 fielding in December 2015 with guidance to the NSA and the Services to implement mitigation plans to resolve suitability problems discovered during the LUTs.
- In February 2016, the KMI PMO changed the original FDD estimate to February 2018, thus triggering a Significant Change.
- KMI Operations issued the Spiral 2, Spin 1 Maintenance Release 1 (MR1) in May 2016. Spin 1 MR2 completed developmental testing in June 2016, and the KMI Configuration Control Board approved Spin 1 MR2 for production in late August 2016.
- The KMI PMO and JITC conducted the government-led DT&E-2 of Spiral 2, Spin 2 capabilities in July 2016. Major problems with Spin 2 capabilities required the KMI PMO to delay the DT&E-2 regression event from August to October 2016.
- JITC conducted no KMI operational testing in FY16, due to Spin 2 schedule delays.
- The DOD Chief Information Officer convened KMI Executive Management Reviews that focused attention on significant problems with the KMI schedule, developer staffing, and shared test infrastructure resources. The KMI PMO, Service stakeholders, and test community met to help orchestrate the integrated Spin 2 and Spin 3 schedule that accounts for KMI development, KMI and EKMS sustainment, shared test infrastructure usage, and operational risk reduction with EKMS message server hardware and software upgrades.
- All Services are fielding KMI Spiral 2, Spin 1; account transitions as of October 2016 are:
  - Army - 97
  - Air Force - 192
  - Navy - 235
  - Defense Agencies - 25
- The Army will accelerate account transitions with the Spin 2 fielding decision projected for late 2017. The Army will be unable to transition all of its Non-secure Internet Protocol Router Network key managers to KMI before December 2017 and will need EKMS extended into 2018. The Navy indicated that some afloat accounts will not transition until 2018 and will need EKMS to accomplish the transition process.

Assessment

- Users are satisfied with Spiral 2, Spin 1 capabilities, performance, and system stability. Functionality improved for the LUT Retest, but some suitability problems remain unresolved.
- KMI Spiral 2, Spin 2 developmental and operational testing is at least 12 months behind schedule, and the program is at risk of not meeting its new FDD in 2018.
- Service users completed the Spin 2 DT&E-2 in July 2016, identifying numerous critical problems, some of which are process and procedural problems related to EKMS-to-KMI transition. PMO regression testing of the fixes to those defects began in September 2016.
- The KMI Spiral 2, Spin 2 test schedule is aggressive and high-risk based on the time required to integrate and test the previous spin's capabilities.
- The KMI PMO delayed the Spiral 2, Spin 2 Operational Assessment due to software integration problems found in the Spin 2 DT&E-2. Additionally, the KMI PMO experienced significant Spin 3 integration and developmental testing delays. Because of these delays, the KMI PMO can only develop, test, and field three of four spins prior to the desired EKMS end-of-life date in 2017.
- Problems observed in previous developmental testing, if not corrected during system development, could adversely affect the system's effectiveness, suitability, or survivability during the KMI Spiral 2, Spin 2 LUT, which the KMI PMO delayed from January 2017 to June 2017.
- The KMI training system (separate from the operational KMI system) has connection and updating problems that effect KMI courses and student training.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed one of the FY14 and FY15 recommendations. The following remain unresolved:
  1. Improve rigor of the KMI software development and regression process to identify and resolve problems before entering operational test events.
  2. Allot adequate schedule time to support test preparation, regression, post-test data analysis, verification of corrections, and reporting to support future deployment and fielding decisions.
  3. Verify increased KMI token reliability through a combination of laboratory and operational testing with

automated data collection from system logs for accurate reliability and usage analysis.

4. Demonstrate a regular maintenance release schedule and resolve the backlog of deficiencies.
5. Ensure that appropriate transition and funding plans are in place to continue development and support fielding efforts beyond FY17 target dates, since all Services will have some accounts that will not transition until FY18.
6. Resolve HBSS version management and re-verification process problems that obstruct autonomous operations.
7. Improve and institutionalize rigorous configuration management, software and security update processes, and version controls to properly sustain KMI.
8. Ensure adequate engineering, second echelon, system administrators, database managers, and NSA/Service Help Desk and transition staffs are available to support surge fielding and long-term KMI sustainment.

- FY16 Recommendations. The KMI PMO should:
  1. Ensure shared test resources are synchronized with competing NSA program and sustainment efforts, and continue to maintain an overall schedule that is executable with coordinated Service support and participation.
  2. Prepare to extend the EKMS end-of-life, as the Navy has indicated that some afloat accounts will not transition until 2018 and will need EKMS to accomplish the transition process. The Army will be unable to transition all of its Non-secure Internet Protocol Router Network key managers to KMI before December 2017 and will need EKMS extended into 2018.
  3. Improve KMI training system connectivity, software updating, and sustainment support for KMI courses and student training.

Next Generation Diagnostic System (NGDS) Increment 1

Executive Summary

- The Next Generation Diagnostic System (NGDS) is a polymerase chain reaction analytical instrument. The Services intend NGDS to provide clinical diagnostic capability to diagnose biological warfare agent (BWA)-related illness and environment sample analysis to identify the presence of BWA in the operational environment.
- BioFire Defense, Limited Liability Corporation (LLC), the major contractor, is conducting Food and Drug Administration (FDA)-approved clinical trials on the NGDS hardware, software, the consumable assay, and analytical methods for BWA-related diseases to support FDA clearance of NGDS for clinical use.
- The Army Test and Evaluation Command conducted an operational assessment of the NGDS May 18 – 27, 2016, at Camp Bullis, Texas.
- Based on an analysis of operational assessment data, deployable medical units equipped with NGDS can analyze clinical specimens and provide timely and accurate information to support medical diagnosis, treatment, and force health protection decisions.
- The NGDS demonstrated 98 percent mission reliability and 98 percent operational availability during the operational assessment.

System

- The NGDS Increment 1 Deployable Component is the FilmArray 2.0 commercial off-the-shelf liquid sample polymerase chain reaction analytical instrument with automated sample preparation.
- The NGDS and the Warrior Panel for biological warfare agent identification will be FDA-cleared for diagnostics use on clinical specimen types.
- The system includes a ruggedized computer, software, ruggedized transport case, optical handheld barcode scanner, optical mouse, power and communication cables, pouch loading module, consumable assays. and an operator's manual with sample protocols.
- The Services intend to use the NGDS Increment 1 Deployable Component in existing microbiology laboratories equipped with common laboratory support equipment such as Class II Bio Safety Cabinet, refrigerator, freezer, level work surfaces, line power sources, lighting, and appropriately trained laboratory personnel and units.

Mission

- Trained clinical laboratory personnel equipped with the NGDS Increment 1 Deployable Component will identify BWAs and infectious diseases in clinical specimens (e.g., blood, sputum, nasopharyngeal swabs) to support medical provider's clinical diagnosis and treatment decisions.
- Trained laboratory personnel equipped with NGDS will identify BWAs in environmental samples to confirm a potential BWA incident and support Force Health Protection decision making.

Major Contractor

BioFire Defense, LLC – Salt Lake City, Utah

Activity

- BioFire Defense conducted FDA-approved pre-clinical trial testing of the NGDS during FY15. It is currently conducting FDA-approved clinical trials on the NGDS hardware, software, the consumable assay, and analytical methods for BWA-related diseases. The FDA will use clinical trial data to determine if the system should be cleared for diagnostic use.
- The NGDS program conducted the following developmental and logistics testing between July 2015 and August 2016:
  - Electromagnetic compatibility testing and Military Standard 810 environmental testing from July to August 2015

- Synthetic DNA material testing to validate its use as a stimulant for operational testing from February to March 2016
- Cooperative Vulnerability and Penetration Assessment cybersecurity testing in April 2016
- Logistics Demonstration in May 2016
- Military Standard 810 follow-on testing in May 2016

• DOT&E approved the NGDS Increment 1 Deployable Component operational assessment plan on May 9, 2016.
• The Army Test and Evaluation Command conducted the operational assessment May 18 – 27, 2016, at Camp Bullis, Texas, in accordance with the DOT&E-approved Test and Evaluation Master Plan and operational test plan.

Assessment

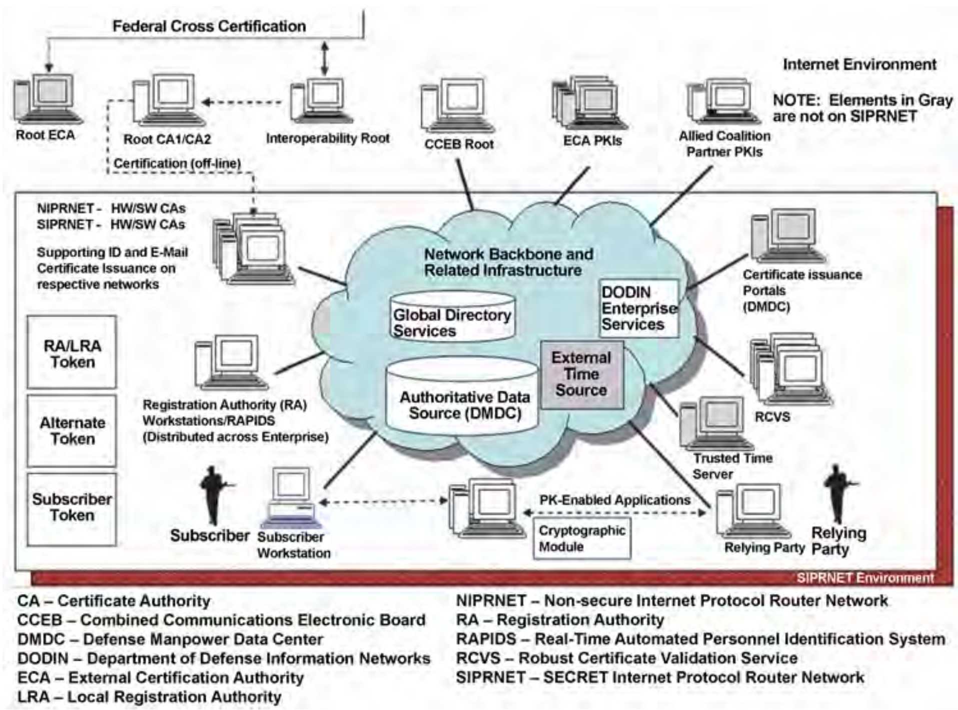
• Based on an analysis of operational assessment data, deployable medical units equipped with NGDS can analyze clinical specimens and provide timely and accurate information to support medical diagnosis, treatment, and force health protection decisions.
• Clinical laboratory personnel are able to prepare and analyze a clinical sample in an average of 68 minutes and correctly report diagnostic results for multiple agents at the same time.
• The NGDS automated sample preparation and analysis process reduces operator sample preparation tasks and minimizes the opportunity for error.
• The NGDS infectious disease diagnostic capability will enable laboratory personnel to maintain proficiency that can be applied should a BWA incident occur.
• The NGDS demonstrated 98 percent mission reliability and 98 percent operational availability during the operational assessment.
• NGDS has cybersecurity vulnerabilities that need to be corrected and re-tested prior to fielding.
• FDA clearance for medical use must be obtained for the NGDS and Warrior Panel prior to fielding.

Recommendations

• Status of Previous Recommendations. There are no previous recommendations for this program.
• FY16 Recommendation.
  1. The program manager should correct cybersecurity vulnerabilities prior to the IOT&E and fielding.

Public Key Infrastructure (PKI) Increment 2

Executive Summary



- DOT&E published a memo in late December 2015 noting that poor Secret Internet Protocol Router Network (SIPRNET) token reliability continues to impede operational missions requiring secure access to SIPRNET, and recommended that the Public Key Infrastructure (PKI) Program Management Office (PMO) address the problem. The PMO recently began issuing two new token types to the field, and deploying to a small set of users an automated token data logging capability to evaluate and improve token reliability. The new token types include a redesigned token from the existing manufacturer and a second source token type based on Common Access Card technology.
- In late February 2016, the PKI Program Manager changed his Full Deployment Decision (FDD) estimate to April 2018, triggering a Significant Change. The program manager subsequently changed his FDD estimate to July 2018.
- The Joint Interoperability Test Command (JITC) conducted a Limited User Test (LUT) of PKI Token Management System (TMS) releases 4.1, 4.2, and 4.3 from July 18 to August 11, 2016. New capabilities under test included Very Important Person (VIP) and Traditional Group, Role-based, and User-Identity tokens; recovery of past encryption keys to a token; TMS monitoring; and automatic failover between the primary and alternate sites. Test results revealed that DOD PKI Increment 2 Spiral 3 Releases 4.1, 4.2, and 4.3 are operationally effective, operationally suitable except for the Advanced Reporting System (ARS), and interoperable. Cybersecurity analyses are ongoing.
- JITC and National Security Agency (NSA) cybersecurity teams conducted a cooperative cybersecurity assessment of TMS in July 2016.
- DOT&E published the PKI TMS Release 4 LUT report in November 2016.
- A persistent cyber opposing force identified a significant PKI vulnerability during a DOT&E-sponsored cybersecurity assessment, and DOT&E is preparing a classified finding memo that will recommend remediations.
- The NSA PKI PMO delayed deployment of the Defense Information Systems Agency (DISA) Integration Lab (DIL), a key aspect of the program's late 2014 post-critical change way ahead. Without the DIL, the PKI Program Manager will continue to deploy potentially immature capabilities directly to the production environment, creating operational risk for users.
- JITC plans to conduct a Spiral 3 FOT&E from April to May 2017.

System

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. DOD PKI supports the secure flow of information across the DOD Information Networks as well as secure local storage of information.
- The SIPRNET TMS's primary mission is to issue tokens and certificates to end users. The private keys are encoded on the token, which is a smartcard embedded with a microchip.
  - The NSA manages TMS with operational support from DISA, which hosts the infrastructure and provides PK enabling support for DOD. TMS uses the Defense Manpower Data Center's Secure Defense Enrollment Eligibility Reporting System (DEERS) as the authoritative data source for personnel data and provides capabilities for token formatting, user registration, token enrollment, token personal identification number reset, token suspension and restoration, token revocation, and encryption private key escrow and recovery.
  - TMS uses commercial off-the-shelf (COTS) hardware and software components using Linux-based operating

systems hosted at the DISA Enterprise Service Centers in Mechanicsburg, Pennsylvania, and Oklahoma City, Oklahoma.
- The NSA deployed PKI Increment 1 on the Non-secure Internet Protocol Router Network (NIPRNET) with access control provided through Common Access Cards. The NSA is developing and deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA deployed Spirals 1 and 2, while Spirals 3 and 4 will deliver TMS enhancements, inventory logistics tools, an enterprise-level alternate token issuance and management system (for system administrators) on the NIPRNET, and an enterprise-level non-person entity (NPE) (e.g., workstations, routers, and web servers) for certificate issuance and system management.

Mission
- Commanders at all levels will use DOD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards or SIPRNET tokens to enable DOD members, coalition partners, and others to access restricted websites, enroll in online services, and encrypt and digitally sign email.
- Military operators, communities of interest, and other authorized users will use DOD PKI to securely access, process, store, transport, and use information, applications, and networks.
- Military network operators will use NPE certificates for workstations, web servers, and mobile devices to create secure network domains, which will facilitate intrusion protection and detection.

Major Contractors
- General Dynamics Mission Systems – Dedham, Massachusetts (Prime)
- 90Meter – Newport Beach, California
- SafeNet Assured Technologies – Abington, Maryland

Activity
- The PKI PMO conducted multiple government-led TMS 4.1 and 4.2 developmental tests to resolve software deficiencies from December 2015 to June 2016.
- DOT&E published a memo in late December 2015 noting that poor SIPRNET token reliability continues to impede operational missions requiring secure access to SIPRNET, and recommended that the PKI PMO address the problem. The PMO recently began issuing two new token types to the field, and deploying to a small set of users an automated token data logging capability to evaluate and improve token reliability. The new token types include a redesigned token from the existing manufacturer (SafeNet) and a second source token type based on Common Access Card technology.
- DOT&E approved the PKI Spiral 3 Test and Evaluation Master Plan (TEMP) Addendum in February 2016.
- The PKI PMO and JITC began writing the Spiral 4 TEMP Addendum in late February 2016. Spiral 4 will support the NIPRNET Enterprise Alternate Token System (NEATS), NPE, and Secure Channel Protocol (SCP) 03 development efforts and testing.
- In late February 2016, the PKI Program Manager changed his FDD to April 2018, triggering a Significant Change. The program manager subsequently changed his FDD estimate to July 2018.
- JITC conducted a LUT of PKI TMS Releases 4.1, 4.2, and 4.3 from July to August 2016. These releases provide TMS privileged users with enhanced management and reporting functions, TMS system administrators with improved monitoring tools, and SIPRNET token end-users with more flexible ways to securely share information through group and role-based tokens. Additionally, TMS 4.3 implements an automated failover capability. TMS 4.1, 4.2, and 4.3 capabilities include:
  - TMS VIP, Traditional Group, role-based, and user-identity token processes and enrollments with encryption, identity, and signing certificate attributes.
  - ARS uses the Pentaho COTS tool to create data-object templates and ad hoc reports.
  - The Nagios COTS tool that provides the DISA system administrators with a system health and monitoring dashboard view of TMS performance metrics, server services, connections, storage, and data files.
- JITC and NSA cybersecurity teams conducted a cooperative cybersecurity assessment of TMS in July 2016.
- DOT&E published the PKI TMS Release 4 LUT report in November 2016.
- A persistent cyber opposing force identified a significant PKI vulnerability during a DOT&E-sponsored cybersecurity assessment, and DOT&E is preparing a classified finding memo that will recommend remediations.
- The PKI PMO plans to conduct developmental testing of TMS release 5.0 and 6.0, starting in December 2016.
- JITC plans to conduct the Spiral 3 FOT&E from April to May 2017.

Assessment
- Developmental testing conducted on the production environment in February, March, and June 2016 resulted in the identification and fixing of 11 high-priority software deficiencies. Four high-priority deficiencies were found during the four-week LUT, not including several high-risk cybersecurity vulnerabilities, which are still being evaluated. PMO delays in software delivery and the need for successive regression testing in the production environment have overtaxed the user community and further compressed the already aggressive Increment 2 schedule.

- Developmental test planning and process improvements since the critical change included an event-driven test approach, regression testing prior to proceeding to operational testing, and involving more Service and agency users in test events.
- From April to June 2016, there were ongoing TMS performance/latency problems impeding certificate issuance and revocation that affected PKI mission operations for all Services and agencies. The PKI PMO reduced those latency and failover problems with the hardware refresh completed at the DISA hosting sites in late June 2016.
- Services and agencies continue to experience SIPRNET token shortages that are a direct result of poor logistics supply planning, high token failure rates, and delays in provisioning and long lead time for new token types. Moreover, a surge of expiring SIPRNET PKI certificates (certificates expire after 3 years) require users to renew their certificates, which involves the time-consuming process of interfacing with a Registration Authority (RA).
- Significant PKI SIPRNET token shortages forced Services to institute rationing for FY16.
- PKI TMS release 4.1, 4.2, and 4.3 LUT assessment:
  - JITC examined TMS VIP, group, and role token processes and enrollments with encryption, identity, and signing certificate attributes. The TMS 4.1 and 4.2 functionality is working properly and provides operational benefits such as methods for encouraging adoption of secure authentication, encryption, and non-repudiation.
  - A new bulk revocation capability has been tested successfully by many Services and agencies, driven by the large stock of returned tokens that require proper handling for termination or reuse.
  - The PMO placed two new token types into circulation to address the poor reliability of existing tokens. JITC has not operationally tested these new token types, and the Services have yet to equip most sites with the required middleware version to utilize the new tokens. The Services are reporting few problems with the new token types.
  - JITC evaluated ARS, which uses the Pentaho tool to create data-object templates and ad hoc reports. The Service RAs stated that ARS is a powerful tool, but they need a tailored instruction guide and more training to better understand how to use ARS.
  - JITC tested TMS release 4.3 and the Nagios COTS tool that provides DISA system administrators with a system health and monitoring dashboard view of TMS performance metrics, server services, connections, storage, and data files. TMS 4.3 implements an automated failover capability, which worked during the LUT. The Nagios tool will be more useful once it is tailored to meet the system administrators' specific system monitoring needs with specific thresholds for generating alerts that are tuned and once the system administrators define the techniques, tactics, and procedures for the tool.
- PKI LUT findings revealed that DOD PKI Increment 2 Spiral 3 Release 4.1, 4.2, and 4.3 are operationally effective, operationally suitable except for ARS, and interoperable. Security data analyses are ongoing.
- PKI LUT results indicated the following:
  - Some users experienced intermittent connectivity problems when enrolling tokens; however, the extent to which this affects their productivity is unclear.
  - TMS granted excessive privileges to Trusted Agents, allowing them to inadvertently renew a certificate rather than simply resetting a Personal Identification Number.
  - While running a report using ARS, one RA discovered approximately 500 active certificates that TMS should have revoked when the RA terminated the associated tokens. This should not have occurred because TMS should automatically revoke certificates when an RA terminates a token.
  - Users liked VIP group tokens, which allow staff members of senior officials to better handle official encrypted email traffic.
  - PKI successfully demonstrated automatic failover between the primary and alternate sites during the LUT after JITC-identified system configuration problems were corrected.
  - DISA system administrators successfully used the Nagios monitoring capability to troubleshoot TMS failures; however, the volume and types of alerts need adjustment to allow system administrators to respond when required.
  - ARS provides a much needed token reporting capability; however, users require more focused training. Default templates for standard data objects (e.g., number of tokens issued per month by Service) would be beneficial to users who do not have access to focused training.
- DISA system administrators identified a TMS-related configuration management problem that prevented automatic failover and complete data replication between the two Enterprise Service Center hosting sites. During the LUT, RAs attempting to run ARS reports during the LUT discovered that the report data were incomplete. The PKI PMO found the root cause and fixed the problem during the test, and subsequent failovers and data replication between sites functioned properly.
- The NSA PKI PMO and DISA delayed deployment of the DIL, a key aspect of the program's late 2014 post-critical change way ahead, due to lack of DIL effort prioritization, funding shortfalls, and hardware procurement problems. Without the DIL, the PKI Program Manager will continue to deploy potentially immature capabilities directly to the production environment, creating operational risk to users.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed one of four previous FY15 recommendations. The following remain:
  1. Develop the Spiral 4 TEMP Addendum in accordance with the redefined PKI Increment 2 Acquisition Strategy to

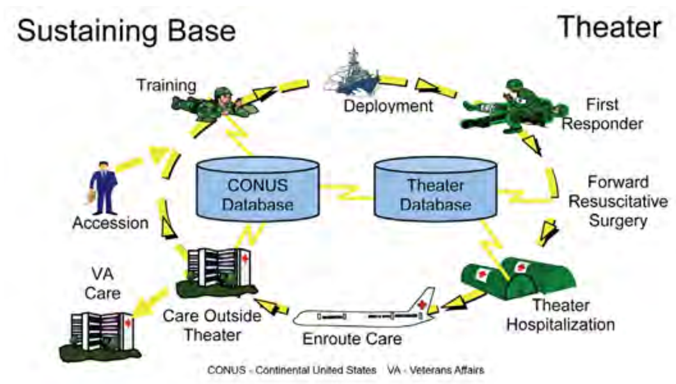
prepare stakeholders for the remaining deliveries, resource commitments, and T&E goals.
2. Define and validate sustainment requirements for PKI Spiral 4 capabilities.
3. Provide periodic reports of token reliability, failure rates, and root cause analyses.

- FY16 Recommendations. The PKI PMO should:
  1. Establish an operationally representative DIL to properly examine TMS and NPE capabilities in a test environment containing realistic token data, interfaces to user test laboratories, and an email server to improve test adequacy prior to deploying capabilities to production.
  2. Implement the cybersecurity mitigating actions from the classified memo.

Theater Medical Information Program – Joint (TMIP-J)

Executive Summary

- The Army Test and Evaluation Command (ATEC) conducted a Multi-Service Operational Test and Evaluation (MOT&E) of Theater Medical Information Program – Joint (TMIP-J) Increment 2 Release 3 (I2R3) that included a cybersecurity Adversarial Assessment from August 13 – 21, 2015. The Air Force Operational Test and Evaluation Center, Marine Corps Operational Test and Evaluation Activity, United States Army Medical Department Board, Air Force Medical Evaluation Support Activity (AFMESA), Marine Corps Tactical Systems Support Activity (MCTSSA), and the Joint Interoperability Test Command (JITC) all participated in the MOT&E. The MOT&E was adequate to assess operational effectiveness, operational suitability, and survivability for the Army, Air Force, and Marine Corps.
- The Commander, Operational Test Force (COTF) conducted Navy OT&E in a test environment aboard the USS *Carter Hall* (LSD 50) while in port at Joint Expeditionary Base, Little Creek, Virginia, and while underway in the nearby Virginia Capes operating area. COTF completed the mission-oriented functional OT&E from November 6 through December 18, 2015, and conducted cybersecurity testing from January 11 – 15, 2016. The Navy OT&E was adequate to support an assessment of survivability, but not adequate to support a full assessment of operational effectiveness or operational suitability for the Navy.
- TMIP-J I2R3 is not operationally effective for the Army, Air Force, and Marine Corps. DOT&E could not fully assess the operational effectiveness of TMIP-J I2R3 for the Navy. The Army and Air Force identified problems in the core mission areas of Health Care Documentation and Medical Command and Control that may pose risks to patient safety and prevent the system from being operationally effective for the Army, Air Force, and Marine Corps until these problems are corrected or mitigated. The Navy collected insufficient samples to determine whether problems reported by other Services in the mission area of Medical Command and Control exist in the Navy implementation of TMIP-J. TMIP-J I2R3 is effective for the Navy in the core Business Process Support mission areas of Health Care Documentation and Preventative Medicine. The three joint interfaces evaluated met the accuracy and timeliness thresholds for interoperability, and network operations were effective for all Services.
- TMIP-J I2R3 is operationally suitable for the Army, Air Force, and Marine Corps. DOT&E could not assess operational suitability for the Navy because positive mission performance results conflicted with negative user opinions from the small number of Navy test participants and the Navy failed to conduct follow-up interviews with TMIP-J I2R3 users during the Navy portion of the MOT&E.



- TMIP-J I2R3 is not survivable. During the Army, Air Force, and Marine Corps MOT&E, cybersecurity test aggressors penetrated the system and gained access to the test patient health records as an insider/nearsider to the system. During the Navy OT&E, cybersecurity test aggressors identified no vulnerabilities with the TMIP-J I2R3 software itself, but did identify vulnerabilities in thr Consolidated Afloat Network and Enterprise Services (CANES) system. The CANES vulnerabilities enabled the cyber aggressors to penetrate TMIP-J workstations.

System

- TMIP-J is a Major Automated Information System that integrates software from sustaining base medical applications into a multi-Service system for use by deployed forces. Examples of integrated applications include the theater versions of the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Defense Medical Logistics Standard Support.
- TMIP-J provides the following medical capabilities:
  - Electronic Health Records
  - Medical command and control
  - Medical logistics
  - Patient movement and tracking
  - Patient data to populate the Theater Medical Data Store (theater database) and the Clinical Data Repository (Continental U.S. database)
- The Services provide their own infrastructure (networks and communications) and computer hardware to host the TMIP-J software.
- TMIP-J consists of two increments. The Program Executive Office fielded Increment 1 in 2003 and is developing Increment 2 in multiple releases with the following fielding dates:
  - Increment 2 Release 1 – fielded in 2009.
  - Increment 2 Release 2 – fielded in 2014.

- Increment 2 Release 3 was the system under test during 2015 and is the final TMIP-J release.
- The Program Executive Office initiated the Joint Operational Medicine Information Systems (JOMIS) program in FY15. This program will replace portions of TMIP-J.

Mission

- Combatant Commanders, Joint Task Force commanders, and their medical staff equipped with TMIP-J can make informed and timely decisions about planning and delivering health care services in the theater.
- Military health care providers equipped with TMIP-J can electronically document medical care provided to deployed forces to support continuity of medical care from the theater to the sustaining base.

Major Contractors

- SAIC – Falls Church, Virginia
- Northrop Grumman – Chantilly, Virginia
- Akimeka LLC, Kihei – Maui, Hawaii

Activity

- ATEC conducted an MOT&E of TMIP-J I2R3 in accordance with the DOT&E-approved test plan from August 13 – 21, 2015. The Air Force Operational Test and Evaluation Center, Marine Corps Operational Test and Evaluation Activity, United States Army Medical Department Board, AFMESA, MCTSSA, and JITC also participated in the MOT&E. ATEC tested the Army and Air Force components of TMIP-J I2R3 at AFMESA, Fort Detrick, Maryland, and Marine Corps portions of TMIP-J I2R3 at MCTSSA, Camp Pendleton, California.
- In August 2015, the Threat System Management Office conducted a cybersecurity Adversarial Assessment for the Army, Air Force, and Marine Corps portions of TMIP-J I2R3 in conjunction with the MOT&E.
- COTF conducted Navy OT&E with the DOT&E-approved test plan, in a test environment aboard the USS *Carter Hall* (LSD 50) while in port at Joint Expeditionary Base, Little Creek, Virginia, and while underway in the nearby Virginia Capes operating area. COTF conducted mission-oriented functional OT&E from November 6 through December 18, 2015, and cybersecurity testing from January 11 – 15, 2016.
- Following the MOT&E, the JOMIS Program Manager developed TMIP-J I2R3 Service Pack 1 (SP1) to correct discovered problems.
- In June 2016, the JOMIS Program Manager completed a TMIP-J I2R3 SP1 developmental test and evaluation regression test and released the system software to the Services for implementation.
- In August 2016, the JOMIS Program Manager completed installation of TMIP-J I2R3 SP1 on the TMIP-J baseline system at Joint Task Force Bravo, Soto Cano Air Base, Honduras.

Assessment

- The MOT&E and the Navy OT&E were adequate to assess survivability for all Services. The MOT&E was adequate to assess operational effectiveness and operational suitability for the Army, Air Force, and Marine Corps, but the Navy OT&E was not adequate to fully assess operational effectiveness and operational suitability.
- TMIP-J I2R3 is not operationally effective for the Army, Air Force, and Marine Corps. DOT&E could not fully assess the operational effectiveness of TMIP-J I2R3 for the Navy.
  - There were no deficiencies in the core mission areas of Patient Movement and Medical Logistics. However the August 2015 MOT&E identified problems in the core mission areas of Health Care Documentation and Medical Command and Control that may pose risks to patient safety and prevent the system from being operationally effective until these problems are corrected or mitigated. Specifically, users must manually enter the same patient data into multiple systems as no automated interface between them exists, increasing the potential for errors or incomplete medical data in one or more systems. The Navy collected insufficient samples to determine whether problems reported by other Services in the mission area of Medical Command and Control exist in the Navy implementation of TMIP-J. TMIP-J I2R3 is effective for the Navy in the Business Process Support mission areas of Health Care Documentation and Preventative Medicine.
  - The three joint interfaces evaluated met the accuracy and timeliness thresholds for interoperability.
  - Network operations were effective for all Services, although there were initial difficulties in establishing tactical communications through supporting Service networks. During the first seven days of the MOT&E, the Army, Air Force, and Marine Corps were unable to exchange data over their very small aperture terminal satellite systems. Service technicians isolated the problem to a network device that was altering packets because of an incomplete security certification. They solved the problem by obtaining a new certification. Satellite communications problems aboard the USS *Carter Hall* delayed testing. Once the Navy fixed these problems, TMIP-J I2R3 data successfully traversed the network while both dockside and underway to perform the mission.
- TMIP-J I2R3 is operationally suitable for the Army, Air Force, and Marine Corps. DOT&E could not evaluate operational suitability for the Navy because positive mission performance

results conflicted with negative user opinions from the small number of Navy test participants, and the Navy failed to conduct follow-up interviews with TMIP-J I2R3 users during the Navy OT&E.

- System administrators responded favorably to survey questions regarding administration of the system.
- User opinion surveys from the Army, Air Force, and Marine Corps confirmed that their respondents liked the system and found it easy to use. They reported a mean score of 70 on the System Usability Scale (SUS), indicating acceptable usability. However, Navy user opinion surveys resulted in a very low mean score of 38, indicating unacceptable usability for medical users aboard the USS *Carter Hall*.
- Army, Air Force, and Marine Corps test participants indicated that the TMIP-J I2R3 supporting documentation was helpful and that they were satisfied with help desk performance. The Army and Air Force did not adequately capture reliability and availability data during the test event, but there were no indications that the system is not reliable or available. The Marine Corps reported an availability of 99.8 percent, which exceeded the 99 percent availability threshold with confidence. The Navy reported 243 hours of system operating time, with no observed failures resulting in an 80 percent lower confidence bound of 151 hours Mean Time Between Operational Mission Failures due to software and 100 percent availability.

- TMIP-J I2R3 is not survivable. During Army, Air Force, and Marine Corps OT&E, cybersecurity test aggressors penetrated the system and gained access to the test patient health records as an insider/nearsider to the system. During the Navy OT&E, cybersecurity test aggressors identified no vulnerabilities with the TMIP-J I2R3 software itself, but did identify vulnerabilities in the CANES hosting platform for TMIP-J I2R3. The CANES vulnerabilities enabled cyber aggressors to penetrate TMIP-J workstations.

Recommendations

- Status of Previous Recommendations. There were no previous recommendations.
- FY16 Recommendations.
  1. The Program Executive Officer of Defense Healthcare Management Systems, in coordination with the Services and the Defense Health Agency Functional Advisory Council, should address problems discovered during the MOT&E.
  2. The Operational Test Agencies should retest TMIP-J I2R3 capabilities in a representative operational environment with operational users to support a final fielding of TMIP-J I2R3.
  3. The Navy should ensure all instances of CANES, on all platforms, are properly patched and configured for cybersecurity and routinely conduct cybersecurity testing of CANES installations.

Army Programs

Army Programs

Army Network Modernization

The FY16 National Defense Authorization Act directed the DOD to conduct a comprehensive assessment of the current and future capabilities and requirements of the Army's air-land, mobile tactical communications and data networks, including technological feasibility, suitability, and survivability. The study encompasses all Army air and land tactical communication systems; developments to date, planned enhancements (primarily programs of record), and potential future developments. Army programs of record include: Warfighter Information Network – Tactical (WIN-T); Mid-Tier Networking Vehicular Radio (MNVR); Handheld, Manpack, Small Form Fit (HMS) Rifleman Radio; HMS Manpack Radio; and Small Airborne Networking Radio (SANR). This report includes initial findings from the assessment to include:

- Capabilities of the currently fielded mobile tactical network
- Current and future operational needs that are not met by the existing capabilities
- Challenges in the Army's network modernization plans with an emphasis on the software-defined radio programs (HMS Rifleman Radio, HMS Manpack Radio, MNVR, and SANR)
- Analysis of software and hardware design concepts to understand root causes of these challenges

The final report is expected to be complete in March 2017. It will include an assessment of which challenges can improve with the current systems, which would require significant redesign of the network or individual systems, whether or not solutions, including technology alternatives, exist.

The Army's goal for its tactical network is to provide higher data rates to the individual user, to transfer voice and data simultaneously, and in the case of WIN-T Increment 1, replace multiple stove-piped systems to allow for a network with open communication within and beyond theater. Demonstrated performance to date of the mobile line-of-sight (LOS) tactical network indicates that it will not meet the Army's operational needs. The software-defined radio programs of record with their Mobile Ad hoc Network (MANET) design have struggled to meet requirements for range, power consumption, and message completion rate (MCR). The network as a whole is limited to between 30 and 40 nodes per channel and therefore requires complex planning and management and restricts unit task reorganization. The network has demonstrated poor survivability in contested electronic warfare environments, which is the primary driver for the Army's network modernization.

Performance shortfalls and the disconnect between the Army's Network Modernization plan and its operational priorities stem from multiple gaps in requirements, software (networking waveforms, network management), and the isolated hardware acquisition strategy. The bandwidth requirements, as defined in the radio requirements documents, are not driven by mission command network priorities, but rather by what the network can supply. Certain shortfalls such as the electromagnetic signature susceptibility are trade-offs in network design that are expected when the choice is the MANET. In that case, the capability to operate stealthily was not an operational priority when the Army originally conceived the network modernization plan. Other performance gaps, like high power consumption and network management complexity, are intrinsic to MANET waveforms. The expectation was that as technology evolved these gaps would narrow and the software-defined radios would ultimately outperform their legacy counterparts. In the meantime, the Army has tied requirements of future networking radios to existing waveforms, which are limited by the performance shortfalls intrinsic to those waveforms.

The hardware acquisition approach is such that the Army retains ownership and responsibility for the waveforms and the radio developers retain the rights to the hardware. Industry competitors who supply radio hardware cannot dictate the optimal implementation of the software; instead, they are expected to compete with the minimal possible technology solution that is the lowest cost and simplest to interoperate with other vendors in the multiple source non-developmental item (NDI) selection. They are continuing to build individual software-defined radios, rather than a functioning, integrated network. The effect on the Army's network is that the current path (future radio requirements, capabilities, and acquisition strategies) will not mitigate the performance shortfalls demonstrated to date. The Army should consider not specifying the waveform in requirements documents but rather allowing industry to compete with integrated end-to-end solutions consisting of the waveform and the radio hardware that are based on realistic threat and mission command data needs.

There is opportunity for the Army to recover performance trade-offs, re-align requirements with operational needs, and pursue technology solutions that could more effectively mitigate these shortfalls. Frequent program restructuring and acquisition delays over the past decade have translated into very few radios fielded to date. Three major tactical radio programs, MNVR, HMS Manpack Radio, and HMS Rifleman Radio, have re-entered source selection to allow for full and open competition. SANR is not scheduled for full-rate production until FY23. WIN-T Increment 2 began full-rate production in 2015, but heavy brigades cannot begin fielding until Armored Multi-purpose Vehicle production in 2021. The notable exception is WIN-T Increment 1, which completed fielding, but is still undergoing product improvements.

PERFORMANCE SHORTFALLS

As implemented, the Army's mobile LOS tactical network design diverges from the original MANET architecture. The original design had an ad hoc number of nodes on a single subnet. The idealized MANET architecture was self-healing and self-forming. The ad hoc features allowed a node to seamlessly self-organize into geographically advantageous partitions within the context of the larger, simpler, inclusive network. MANET waveforms include Soldier Radio Waveform (SRW), Wideband Networking Waveform (WNW), and Highband Networking Waveform (HNW). This architecture has been replaced by multiple defined subnets. The effect of breaking the network into a number of small subnets places an increased burden on network planners who must manually configure each user device to constrain communication to a specific set of nodes. Units are dependent on contractors to design and configure this complex network.

Electromagnetic Signature Vulnerability

In comparison to legacy systems, the Army's networking radios are more susceptible to electronic surveillance. Legacy push-to-talk radios limit their electromagnetic expression to those instances when user data need to be transmitted. Networking radios are constantly emitting in order to discover neighbors, maintain connectivity, and evaluate link conditions. Reducing the signal strength to mitigate this vulnerability requires reducing the transmit power of the signal, while to improve the LOS range requires increasing the power. Given that the Capabilities Production Documents (CPDs) for the software-defined radios currently require the radios to operate MANET waveforms, programs as currently defined cannot expect to produce systems with a reduction in electromagnetic signature.

Shorter Line-of-sight (LOS) Range than Legacy Radios

Range expectations for tactical networking radios are that they meet or exceed those set by their legacy counterparts. Reductions in range would require the Army to reconsider how they conduct tactical combat operations. Progress in radio frequency technology has not translated into better range performance for networking radios. This can be attributed to the constraints under which software-defined radios running SRW or WNW are operating relative to a straightforward Single Channel Ground Air Radio System (SINCGARS) implementation. SRW and WNW operate at higher frequencies than SINCGARS. The higher operating frequencies are more susceptible to range-limiting losses in even benign terrain conditions.

The exchange of information over a MANET is dependent on the health of the direct link between two nodes, the distance between them, and the complex process by which the two communicate. A node must take the time to "join" the network, be recognized by other members, and participate in extensive routing optimization and maintenance before actual data are transmitted or received. Since the nodes are mobile, network formation is an ongoing process, rather than a problem solved at the outset of a mission. As a result, the effective range of a node in a network is limited by a number of factors, (and very difficult to quantify in dynamic conditions). MCR is tied to the node's dynamic membership in the network, rather than the instantaneous condition of a link at the time a message is sent.

Network Complexity

The network is difficult to establish and maintain. Network components, including mission command systems, network manager and the radios, are challenging to use. The value added in having an integrated network to enhance mission command is diminished due to pervasive task complexity. Additionally, the Army is challenged to achieve and maintain user proficiency. Units are dependent upon contractors to plan and support the integrated network. Thus, the Army has implemented the MANET waveforms (WNW, SRW, and HNW) as pre-configured and rigid networks. This architecture has resulted in increased time and complexity required to execute task reorganization, when a unit is attached to a new headquarters. Presently, when unit task reorganization is required, a new network plan has to be created and loaded on to the radios.

High Power Consumption

The Army's software-defined radios have not benefited from technology innovations with respect to power consumption. The fields of battery technology, software-defined power management, improved circuit design, and microfabrication techniques have led to significantly less power needed to operate hardware. Soldiers are burdened with carrying and charging batteries to support dismounted radios. Mounted radios require vehicles to operate more hours per day than legacy radios, precluding the ability to perform silent watch missions and increasing the logistics support burden with increased fuel and vehicular maintenance requirements.

The root cause of the discrepancy can be traced to the design of the MANET radios themselves. Unlike legacy systems that only expend power when the warfighter is communicating, the software-defined radios are operating at near-maximum energy all the time because they must be constantly transmitting and receiving in order to maintain the network, and their presence on it, even when there is no need to transmit any voice or data messages. In the current designs, the best way to minimize the power expended during operation is to leave the network by turning off the radio. In the case of the dismounted HMS Manpack radio, soldiers observed high external temperatures during FOT&E — a common outcome of prolonged operation of high-power devices.

Low Message Completion Rate (MCR)

MCR is a measure of both the functionality of the networking software (i.e., its ability to correctly transmit, route, and parse messages), and the radio frequency connectivity of the underlying links. The current software-defined radios have not demonstrated their requirements for MCR. The demonstrated MCR for situational awareness messages is lower than for command and control messages. Situational awareness messages consist of position location information and other messages related to battlefield entities, e.g. hazard and obstacle map icons that are automatically generated by Joint Battle Command – Platform (JBC-P). Situational awareness messages are transmitted once, and if they do not reach their destination, are dropped. Command and control messages, because of their higher priority, are programmed to keep retransmitting until the sender receives an acknowledgement of receipt.

The low MCR for situational awareness messages can be attributed to the design of the network. In moving away from the original MANET construct into multiple small subnets, the network lost its resiliency of allowing messages to make multiple hops through any node in its immediate proximity. To avoid consuming the available bandwidth, the number of nodes that a message can hop through is limited to those on its subnet even when there may be other nodes in LOS range. Not able to find a route through the network, it drops the situational awareness message causing the blue picture to be stale or inaccurate.

Absence of Anti-Jamming Capability

Two of the Army's principal LOS networking waveforms, SRW and WNW, have not demonstrated their effectiveness against a jamming threat. Anti-jamming techniques involve sophisticated algorithms that consume more bandwidth and produce reduced data rates in return. This would further reduce connectivity and MCRs for waveforms that cannot meet requirements under more benign conditions (open terrain and no jamming). The SRW and WNW standard modes of operation are not intended for a contested electronic environment. SRW's electronic warfare mode offers some jamming resistance but only at reduced data rates. The Army does not intend to use the electronic warfare mode. WNW has an anti-jam mode of operation intended to provide a more robust signal, albeit at lower data rates. Neither the SRW electronic warfare mode nor the WNW anti-jam mode has been demonstrated in an operational test environment. Given the poor performance in benign conditions, the additional constraints added by anti-jam algorithms may make an anti-jam mode not viable without re-investment in the design of the network approach as a whole.

Limited Scalability

To work effectively, the current networking waveforms limit the network to 30-40 nodes per channel. To operate the network with more than 40 nodes requires the MANET to use all the overhead bandwidth establishing and maintaining connectivity among nodes rather than sending and receiving voice or data communications. As currently configured, the radios continue to run software with ad hoc routing algorithms, but the Army has planned and configured the network to prevent ad hoc connectivity by restricting the number of nodes on a particular subnet, and in some cases, constraining exactly which nodes the data could hop through and which other nodes are retransmission vehicles.

REQUIREMENTS AND ACQUISITION APPROACH

The Army has tied the software-defined radio requirements to the existing waveforms for MNVR, HMS Manpack Radio, HMS Rifleman Radio, and SANR. Through this approach, the Army hoped to enhance competition among hardware developers and ensure waveform interoperability across different host systems. Radio capabilities will be limited by the electromagnetic signature susceptibility, high power consumption, low MCR, and network complexity, which are all performance shortfalls intrinsic to the MANET waveforms.

The network requirements are not consistent with the Army's operational needs. The bandwidth requirements, as defined in the radio CPDs, are not driven by mission command network priorities. They are based on what the network can supply rather than how much data are needed at each echelon. The data requirements drive the requirement to operate in higher operating frequencies and are a trade-off with LOS range performance.

The Army's requirements for its tactical networks do not take into account the evolving threat capable of advanced electronic warfare. While the requirements remain rooted in MANET waveforms as currently implemented, the networking solutions will continue to lack sufficient anti-jamming features to mitigate against the effects of electronic attack and remain effective. Direction-finding systems will threaten the survivability of soldiers and host platforms.

The current acquisition approach for HMS Rifleman, HMS Manpack, MNVR, and SANR is a modified NDI in which the Army is retaining ownership and responsibility for the waveform and network manager, and the radio developer is retaining rights to the hardware. Hardware and software developers lack the design control necessary to implement new technology solutions. Hardware contractors have no financial incentive to integrate new technology if the Army's requirements force them to run waveforms that cannot take advantage of those capabilities. In some cases, the contractor may already have its own commercial off-the-shelf waveform optimized for its advanced hardware platform, but may instead opt to deliver a less capable hardware system that better suffices the Army's waveform requirement

Though the government-run reference integration labs continue to make incremental improvements to the Army's networking waveforms, the fundamental design of these waveforms remains rooted in the MANET protocols and hardware functionality of the early 2000s. Since the waveforms were originally developed, research has produced routing protocols that are inherently more scalable and power efficient. Hardware capabilities have similarly advanced, enabling improved signal processing and greater spectrum efficiency. While the commercial sector has widely adopted many of these capabilities, the Army's waveform development and hardware acquisition strategies lack the agility to do so in a timely and efficient manner.

Given these barriers to technology integration, the current acquisition strategy is detrimental to delivering an effective, suitable, or survivable piece of operational equipment to the warfighter. The Army cannot hold the most critical technological element of the radio — the waveform — constant, and at the same time, expect hardware partners to demonstrate sweeping advancements in capabilities. The Army should consider not specifying the waveform in requirements documents but rather allowing industry to compete integrated solutions of the waveform and the radio hardware based on realistic threat and mission command data needs.

PATH FORWARD

Frequent program restructuring and acquisition delays have translated to very few radios fielded to date. To date, the Army has procured less than 10 percent of its full procurement goal. HMS Rifleman Radio has fielded 7 percent of its procurement goal and has re-entered source selection to allow for full and open competition. The remaining tactical radio programs (MNVR and HMS Manpack) are in the early stages of source selection for full and open competition. WIN-T Increment 2 went into full-rate production in 2015, but heavy brigades cannot begin fielding until Armored Multi-purpose Vehicle production in 2021. The notable exception is WIN-T Increment 1, which completed fielding, but is still undergoing product improvements so there is still opportunity for technology injection.

In addition to limited fielding, several aspects of network design are still being deliberated. The Army will conduct an Analysis of Alternatives to the current mid-tier networking solution, MNVR operating WNW. A departure from WNW would represent a major shift in the Army's network plan, affecting not only MNVR, but also SANR, the Army's future aerial networking radio. With network design still being conceptualized and SANR NDI activities yet to start, a clear opportunity exists to influence the direction of the aerial tier.

There is opportunity for the Army to recover performance trade-offs, re-align requirements with operational needs, and pursue technology solutions that could more effectively mitigate these shortfalls. Regardless of the extent to which the Army's networking radios have been fielded or procured, to adapt to the changing threat landscape, a re-direction from the current path is necessary. In order to adapt to these threats the Army will need to adopt new technology (hardware and waveforms) and confront trade-offs in performance.

Network Integration Evaluation (NIE)

The Army conducted one NIE during FY16. NIE 16.2 was conducted in April and May 2016 at Fort Bliss, Texas. In a change from previous years, instead of conducting two NIEs a year to support test and evaluation, the Army conducted a single NIE. Beginning in FY16, the Army is devoting one NIE a year to operational testing and using another annual event, the Army Warfighting Assessment, for experimentation and force development. The first Army Warfighting Assessment was conducted at Fort Bliss in October 2015.

The purpose of the NIEs is to provide a venue for operational testing of Army acquisition programs, with a particular focus on the integrated testing of tactical mission command networks. The Army also intends the NIEs to serve as a venue for evaluating emerging capabilities. These systems, termed by the Army as "systems under evaluation," are not acquisition programs of record, but rather systems that may offer value for future development.

The Army's intended objective of the NIE – to test and evaluate network components in a combined event – is sound. The NIE events allow for a more comprehensive evaluation of an integrated mission command network than is possible through piecemeal evaluations of individual network components.

NIE 16.2
During NIE 16.2, the Army conducted a Limited User Test (LUT) for Warfighter Information Network – Tactical (WIN-T) Increment 3 Network Operations/Net Centric Waveform and an LUT for Spider Increment 1A. In addition, the Brigade Modernization Command conducted an operational assessment of the Mid-Tier Networking Vehicular Radio (MNVR). Individual articles providing assessments of WIN-T, Spider, and MNVR can be found separately in this annual report.

NIE ASSESSMENT

NIE 16.2 was the tenth such event conducted to date. NIEs have been an excellent venue for conducting operational tests of network acquisition programs.

Dedicated Test Unit. Since the first NIE in July 2011, the 2nd Brigade Combat Team, 1st Armored Division has served as the dedicated NIE test unit. Having a dedicated test unit stationed at Fort Bliss, Texas, has been a critical element in successful operational testing conducted during NIEs. It has made the planning and execution of complex brigade-sized operational tests of Army networks much more effective than would be the case if new test units were selected for each event. Past experience demonstrates that having a dedicated test unit enables good operational testing. Due to its experience and the organizational learning that has occurred over time, the dedicated NIE test brigade has shown that it is more attuned to incorporating new systems into its formation for testing than has been the case with one-off test units. As a result, the system under test receives a robust evaluation.

A dedicated test unit is desirable in that it relieves the stress on the Army to designate a test unit of appropriate size each time an operational test is on the schedule for a given program. Some tests require large-scale units up to brigade in size and, when testing command and control systems, sometimes even require a division headquarters element. It is not uncommon to require a brigade combat team-sized or battalion-sized unit. Having a dedicated test unit of a mixed composition enables all of those requirements to be met at one place.

Another aspect of good operational testing is a capable opposing force (OPFOR). The dedicated test brigade has been very proficient in creating this OPFOR. Good operational testing requires an aggressive, adaptive threat unit intent on winning the battle in order to adequately stress the system under test and to fully understand its capabilities. A realistic demanding OPFOR requires capabilities which are not easily assembled and integrated. These capabilities include electronic warfare and cybersecurity threats as well as a mix of heavy and light forces. In particular, the integration of electronic warfare and cyber capabilities into an OPFOR requires practice and is not easily replicated by new units tasked to conduct an OPFOR operational testing mission. The units permanently assigned to conduct the NIEs have, over time, demonstrated the ability to employ an effective OPFOR with a variety of combat multipliers to include electronic warfare and cyber-attack. This OPFOR capability has grown increasingly sophisticated and can be readily adapted to reflect new real-world threat capabilities. This capability may not easily be replicated by a rotational brigade.

For operational reasons unrelated to test and evaluation, the Army has removed 2nd Brigade Combat Team, 1st Armored Division from its mission as the dedicated NIE test unit and has decided to no longer provide a dedicated test unit. This is unfortunate from an operational test and evaluation perspective and, for reasons noted above, the quality of future NIE execution may suffer.

Threat Operations. One of the most significant benefits of NIEs has been the extensive incorporation of threat information operations, such as electronic warfare and computer network operations. Nowhere else has the Army routinely integrated this level of threat capability in either a testing or a training venue. As a result, NIEs have provided numerous insights with respect to operations in this type of threat environment. This capability should be retained and upgraded, as necessary, in future NIEs.

One challenge associated with providing these threat capabilities is cost. They are expensive to provide. The programs of record – or "systems under test" – have borne the cost despite not being funded for these capabilities in their test and evaluation budgets. This has created a funding mismatch before every NIE. The Army should consider centrally funding NIE threat operations to relieve the cost burden on the programs undergoing formal operational testing. This makes particular sense given that the benefits accrue to many of the other systems undergoing some sort of assessment during NIEs, such as "systems under evaluation" and risk reduction events.

Instrumentation and Data Collection. The Army should continue to improve its instrumentation and data collection procedures to support operational testing. For example, the Army Test and Evaluation Command (ATEC) should devote increased effort towards developing instrumentation to collect network data to support WIN-T operational test and evaluation. WIN-T instrumentation has not been adequate to support a thorough evaluation. Improvements are needed with respect to Simple Network Management Protocol polling and Internet Protocol-packet capture and matching. ATEC should also devote effort towards developing instrumentation to collect network data for dismounted radios, such as the Manpack radio. Additionally, the Army needs to place greater emphasis on the use of Real-Time Casualty Assessment instrumentation – an essential component of good force-on-force operational testing – such as that conducted at NIEs. A Real-Time Casualty Assessment is intended to accurately simulate direct and indirect fire effects for both friendly and threat forces. Finally, the Army should continue to refine its methodology for the conduct of interviews, focus groups, and surveys with the units employing the systems under test.

NETWORK PERFORMANCE OBSERVATIONS

The following are observations of tactical network performance during NIEs. These observations focus on network performance deficiencies that the Army should consider as it moves forward with integrated network development.

Network Implementation Challenges. Significant questions remain as to how the network will be implemented in each of the three types of maneuver brigade combat teams (Armored, Infantry, and Stryker). For example:

- Armored Brigade Combat Team Integration. It is not clear how the desired tactical network will be incorporated into heavy brigades, as the challenge of integrating network components into tracked combat vehicles remains unresolved. Due to vehicle space and power constraints, the Army has yet to integrate desired network capabilities into Abrams tanks and Bradley infantry fighting vehicles. For example, at the company level it will be some years before the Manpack network radio will be installed on Abrams tanks and Bradley infantry fighting vehicles. Additionally, it is not clear how the mid-tier tactical network will be established at company level, given that the MNVR radio will not be integrated on either of these vehicles. Implementation of the WIN-T network into the Armored Brigade Combat Team is also some years away, as it is dependent upon successful development and fielding of the Armored Multipurpose Vehicle Mission Command variant.
- Infantry Brigade Combat Team Integration. Integration of the tactical network into an Infantry Brigade Combat Team has not been adequately evaluated in a light infantry unit assigned to the NIE test unit. Integration of the network into the light forces will be challenging given the limited number of vehicles in the Infantry Brigade Combat Team. Most of the key network components, such as Joint Battle Command – Platform, are hosted on vehicles. The challenge of linking into the tactical network is particularly acute at company level and below, where light infantry units operate dismounted. Without a vehicular network node, dismounted units cannot connect to the network above company level.

Networking Waveforms. The Army is committed to using networking waveforms – such as the Soldier Radio Waveform and Wideband Networking Waveform – to implement a networked tactical communications network. While networked communications at lower tactical levels may create enhanced operational capability, the use of networking waveforms brings negative attributes which need to be fully evaluated and understood. For example, networking waveforms, due to their higher frequencies, have shorter ranges and are more affected by terrain obstructions compared to the legacy Single Channel Ground and Airborne Radio System waveform. Networking waveforms and the corresponding software-defined radios were conceived to support data intensive capabilities such as real time video. Such capabilities require high bandwidth, and hence high frequencies, at the cost of shorter ranges. The Army should re-examine whether the current radio and waveform programs best meet the operational needs of maneuver commanders. One clear lesson from previous NIEs is that the two most critical network needs for maneuver commanders at battalion and below are reliable voice communications and GPS-supplied position location information. These needs may be met by a network with much lower bandwidth but increased operating ranges.

Complexity of Use. Network components, including mission command systems and elements of the transport layer, remain very complex to use. The current capability of an integrated network to enhance mission command is diminished due to pervasive task complexity. It is challenging to achieve and maintain user proficiency. Units remain dependent upon civilian field service representatives to establish and maintain the integrated network. This dependency corresponds directly to network complexity of use.

Survivability. An integrated tactical network introduces new vulnerabilities to threat countermeasures – such as threat computer network attacks – and the ability of a threat to covertly track friendly operations. Since networked communications are constantly emitting, they are much more vulnerable to threat electronic direction finding.

The Army should continue to improve its capability to secure and defend its tactical network. The Army should ensure that division and brigade-level cybersecurity teams are appropriately manned and trained.

Air-Ground Communications. The Army has yet to equip its rotary-winged aircraft with radios capable of operating in the same network as ground forces at the company level and below. This remains an important operational gap.

Abrams M1A2 System Enhancement Program (SEP) Main Battle Tank (MBT)

Executive Summary

- In December 2015, the Army conducted a live fire user test event with the Common Remotely Operated Weapon System – Low Profile (CROWS-LP). CROWS-LP demonstrated no degradation to performance over the CROWS II in powered mode. Crews were also able to engage targets effectively in manual mode, an improvement to CROWS II where the height of the weapon hindered accuracy.
- In June 2016, the Army conducted a User Beta Test for Version 4.6 of the Abrams software. There were unexplained accuracy problems with the M829A4 service rounds during the test. The Program Office initiated the investigation of vehicle software, ammunition type, and gun tube wear as potential causes.
- DOT&E approved the Operational Test Agency test plan for the LFT&E of the M1A2 System Enhancement Program Version 3 (SEPv3) Engineering Change Proposal (ECP) la Turret Half-Bustle Ammunition Vulnerability Test Phase I in June 2016. The test is scheduled to start January 2017.
- The Army continued developmental and verification testing to characterize the performance of the M1A2 SEPv3 Next Evolutionary Armor (NEA) against multiple, operationally realistic threats. DOT&E is working with the Army to utilize data from ongoing test phases to support its final assessment of M1A2 SEPv3 survivability against existing and emerging threats in FY20.

System

- The M1A2 SEP Version 2 (v2) and M1A2 SEP Version 3 (v3) are tracked, land combat, assault weapon systems designed to possess significant survivability, shoot-on-the-move firepower, joint interoperability (for the exchange of tactical and support information), and a high degree of maneuverability and tactical agility. The Army intends the M1A2 SEPv2 and M1A2 SEPv3 to enable the crew to engage the full spectrum of enemy ground targets with a variety of point- and area-fire weapons in urban and open terrain.
- The M1A2 SEPv2 is currently fielded. It upgrades the M1A2 SEP by providing increased memory and processor speeds, full color tactical display, digital map capability, compatibility with the Army Technical Architecture, improved target detection, recognition, and identification through incorporation of second generation Forward Looking Infrared technology and electronics and crew compartment cooling through the addition of a thermal management system.
- The Abrams M1A2 SEPv3 fielding is planned for FY20. The M1A2 SEPv3 is an upgrade to the M1A2 SEPv2. The upgrades include the following:

Common Remotely Operated Weapon Station-Low Profile (CROWS-LP)

M1A2 SEP

  - Power generation and distribution to support power demands of future technologies.
  - Network compatibility.
  - Survivability against multiple threats by incorporating NEA, a new underbody IED kit, and other vulnerability reduction measures to reduce the tank's vulnerability to IEDs. These measures include redesigned crew seating, additional floor stiffeners, hardware to provide lower limb protection, and changes in the material and dimensions of internal structural supports.
  - Lethality by providing the ability for the fire control system to digitally communicate with the new large caliber ammunition through use of an Ammo Data Link.
  - Energy efficiency (sustainment) due to the incorporation of an auxiliary power unit.
- The M153A1E1 CROWS-LP is an ECP integration onto the M1A2 SEPv2. The system addresses visibility concerns associated with the existing M153 CROWS II by relocating the sights and laser range finder to the side of the weapon and ammunition box rather than under the weapon, reducing the system height by 10 inches. The ECP includes upgraded software.
- The M1A2 SEP MBT utilizes 120 mm main gun rounds to defeat enemy targets.
  - The XM1147 Advanced Multipurpose (AMP) Round, which is currently in development, is a 120 mm

munition fired utilizing an ammunition datalink-equipped Abrams MBT. The round is optimized for use in urban environments in direct support of assaulting infantry. The Army intends the round to have three defeat modes including Point Detonate (PD), Point Detonate Delay (PDD), and airburst. It will be used to defeat a combination of targets including anti-tank guided missile teams, dismounted infantry, double reinforced concrete wall, light armor, bunkers, obstacles, and armor.
- The M829A4, which was fielded in 2014, is an Armor-Piercing, Fin-Stabilized, Discarding Sabot, 120 mm line-of-sight kinetic energy cartridge. It is the materiel solution for the Abrams' lethality capability gap against threat vehicles equipped with third-generation explosive reactive armor.

Mission

- Units equipped with the M1A2 SEP MBT enable Army combined arms teams to close with and destroy the enemy by fire and maneuver across the full range of military operations.
- The Army intends the M1A2 SEP MBT to defeat and/or suppress enemy tanks, reconnaissance vehicles, infantry fighting vehicles, armored personnel carriers, anti-tank guns, guided missile launchers (ground and vehicle mounted), bunkers, dismounted infantry, and helicopters.

Major Contractor

General Dynamics Land Systems – Sterling Heights, Michigan

Activity

- All testing was conducted in accordance with a DOT&E-approved test plan.
- In December 2015, the Army conducted a live fire user test event with the CROWS-LP. Four tank commanders fired 80 different scenarios and approximately 18,000 rounds during the event at Aberdeen Proving Ground, Maryland.
- In June 2016, the Army conducted a User Beta Test for Version 4.6 of the Abrams software. This software version provides full functionality for the CROWS-LP, the Ammunition Data Link required to support the M829A4 kinetic energy round, and integration for the Joint Chemical Agent Detector.
- In June 2016, DOT&E approved the Operational Test Agency test plan for the LFT&E of the M1A2 SEPv3 ECP la Turret Half-Bustle Ammunition Vulnerability Test Phase I.
- In FY16, the Army continued testing to characterize M1A2 SEPv3 armor performance against multiple threat types under the auspices of NEA, a separate materiel development verification and production effort. DOT&E is following the NEA development and verification program to leverage all relevant data to support the M1A2 SEPv3 survivability assessment. The Army plans to continue testing to characterize NEA and explosive reactive armor performance, vulnerabilities associated with stowed ammunition, and underbody IED protection in FY17.

Assessment

- During the live fire test event, CROWS-LP demonstrated no degradation to performance over the CROWS II in powered mode. Crews were also able to engage targets effectively in manual mode, an improvement to CROWS II where the height of the weapon hindered accuracy.
- There were unexplained accuracy problems with the M829A4 service rounds during the User Beta Test for Version 4.6 of the Abrams software. Crews reported an increase in firing system faults compared to home station vehicles operating on the current software version. The Army is currently conducting a test-based, root cause analysis of the accuracy issue. DOT&E is overseeing these diagnostic tests and analyses and will amend the DOT&E M829A4 report if the test series reveals deviations in originally reported ammunition effectiveness/lethality.
- DOT&E continues to assess data resulting from the Army's ongoing efforts to characterize the protection provided by NEA against expected, operationally-realistic threats. DOT&E will leverage all relevant vulnerability test data from the armor characterization and underbody IED test phases and evaluate all modeling and simulation tools available to support an FY20 final assessment of the tank's survivability to current and expected threats.

Recommendations

- Status of Previous Recommendations. There are no previous recommendations.
- FY16 Recommendations. None.

AH-64E Apache

Executive Summary

- The Army submitted an AH-64E Version 6 Test and Evaluation Master Plan (TEMP) dated October 19, 2016, for OSD approval. The purpose of the TEMP is to support the FOT&E II of the Version 6 AH-64E and a subsequent Post-Full-Rate Production Cut-in Review. The TEMP adequately addresses the operational, cybersecurity, and live fire portions.
- The Director approved the TEMP on November 9, 2016.

System

- The AH-64E is a modernized version of the AH-64D Attack Helicopter. The Army intends to sustain the Apache fleet through the year 2040. The AH-64E is organized in Attack/Reconnaissance Battalions assigned to the Combat Aviation Brigades. Each Battalion has 24 aircraft.
- The Army redesignated the AH-64D Apache Block III as the AH-64E in September 2012.
- The AH-64E's advanced sensors, improved flight performance, and ability to integrate off-board sensor information provide increased standoff and situational awareness in support of the joint force.
- The AH-64E is fielded in two Versions (1 and 4) with a future Version 6 planned in 2017.
- The major Version 1 AH-64E capability improvements included:
  - The ability of the aircrew to control the flight path and the payload of an Unmanned Aircraft System
  - Improved aircraft performance with 701D engines, composite main rotor blades, and an improved rotor drive system
  - Enhanced communication capability, which includes satellite communication and an integrated communication suite to meet global air traffic management requirements
- Version 4 AH-64E retained Version 1 capabilities and added hardware and software for Link 16 network participation.
- The future Version 6 will add multiple enhancements to include:
  - Radar Frequency Interferometer (RFI) passive ranging
  - Fire Control Radar range extension
  - Cognitive Decision Aiding System
  - Maritime Targeting mode
  - Modernized Day Sensor Assembly with color and high definition displays
- The Army acquisition objective is to procure 690 AH 64E aircraft: 634 remanufactured and 56 new build aircraft.

Mission

The Joint Force Commander and Ground Maneuver Commander employ AH-64E-equipped units to shape the area of operations and defeat the enemy at a specified place and time. The Attack/Reconnaissance Battalions assigned to the Combat Aviation Brigade employ the AH-64E to conduct the following types of missions:

- Attack
- Movement to contact
- Reconnaissance
- Security

Major Contractors

- Aircraft: The Boeing Company Integrated Defense Systems – Mesa, Arizona
- Sensors and Unmanned Aircraft System datalink: Longbow Limited – Orlando, Florida, and Baltimore, Maryland

Activity

- The Army submitted an AH-64E Version 6 TEMP dated July 29, 2016, for OSD approval in September 2016. The purpose of the TEMP is to support the FOT&E II of the Version 6 AH-64E and a subsequent Post-Full-Rate Production Cut-in Review. The Army submitted this particular TEMP as a draft for ongoing developmental testing.
- The Army resubmitted an updated version of the TEMP, dated October 19, 2016. The TEMP adequately addresses previous shortcomings from the July version of the TEMP to include operational, cyber, and live fire portions.
- The Director approved the TEMP on November 9, 2016. The Apache Program Management Office (PMO) established

a contract with Boeing that began in April 2015 to address cybersecurity deficiencies from FOT&E I. The Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) are planned for FOT&E II.

Assessment

- Version 4 AH-64E and its interfacing systems have potentially significant cybersecurity deficiencies. Further testing of the AH-64E embedded systems is necessary to determine the significance of the deficiencies.
- Version 4 AH-64E embedded systems are vulnerable to cyber penetration attacks. The AH-64E has been selected by Headquarters, Department of the Army G3/5/7 as one of the five systems to complete an evaluation of cyber vulnerabilities to comply with the National Defense Authorization Act Section 1647 directive. Additionally, the PMO has scheduled a CVPA conducted by the Army Research Laboratory/Survivability Lethality Analysis Directorate for January 2017 and an AA planned for October 2017 as part of FOT&E II.

Recommendations

- Status of Previous Recommendations. The Army has addressed some recommendations from the FY14 annual report. The following recommendations have not been fully implemented:
  1. Improve infrared countermeasures performance, upgrade radar- and laser-warning systems, and improve integration of aircraft survivability equipment on the Version 4 AH-64E.
  2. Address demonstrated cybersecurity vulnerabilities. Plan and conduct unconstrained exploitation of vulnerabilities during adversarial cybersecurity testing.
- FY16 Recommendations. None.

Army Integrated Air & Missile Defense (IAMD)

Executive Summary

- Army Integrated Air and Missile Defense (AIAMD) is a command and control system that will enable an integrated air and missile defense (AMD) system of systems.
- In January 2016, the Army conducted developmental testing of AIAMD that included a Cooperative Vulnerability and Penetration Assessment and missile flight tests. Also, the Army conducted an AIAMD Limited User Test (LUT) in March through May 2016, which included sustained operations to assess system reliability, two missile flight tests, and hardware-in-the-loop (HWIL) events to assess effectiveness and suitability.
- During the HWIL events, operators' assessment was limited to basic air defense missions because of software immaturity and instability, as well as a lack of training for operators on new equipment and new capability operations.
- The IAMD Battle Command System (IBCS) software is neither mature nor stable, as evidenced in numerous software problem reports. This precludes a full assessment of capabilities. Also, software immaturity contributed to the AIAMD Engagement Operations Center's (EOC) reduced reliability; operator workstations often became sluggish or ceased to operate
- AIAMD was unable to effectively operate on the Link 16 network.
- AIAMD system setup, operations, and maintenance technical manuals were incomplete or inadequate.

System

- AIAMD is a command and control system that integrates sensors, weapons, and a common mission command capability across an integrated fire control network (IFCN) to provide a single air picture.
- The IBCS provides the capabilities to control and manage AIAMD-enabled sensors and weapons.
- AIAMD's IBCS will replace and enhance Patriot Data Information Link communication structure, integrate with the currently fielded Sentinel air surveillance sensors, and improve command and control of missile employment.
- The IBCS includes the EOC, hardware interface kits, and IFCN Relays.
  - EOCs provide the operating environment for all levels (battalion and battery) of employment. They will be equipped with IBCS software that enables operators to monitor, interface with, and direct sensor employment and engagement of air threats.
  - Hardware interface kits connect IBCS with the current Patriot and Sentinel missiles, and will incorporate future AMD capabilities to support engagement of air threats. The IFCN is the primary organic communications infrastructure for AIAMD system of systems and provides the capability for fire control connectivity and distributed operations.
  - The IFCN Relay provides a mobile IFCN communications node with an interface kit which extends connectivity to remote launcher and sensor platforms.

Mission

- Army commanders will use AIAMD to provide timely detection, identification, monitoring, and (if required) engagement of air threats (e.g. aircraft, cruise missiles, ballistic missiles, rockets, artillery, and mortars) in an assigned area of responsibility.
- AMD forces deploy to provide active protection for the following:
  - Air defense of the homeland
  - Air defense of priority critical assets and locations
  - Air defense of forces

Major Contractors

- Northrop Grumman – Huntsville, Alabama
- Raytheon – Huntsville, Alabama, and Andover, Massachusetts
- Lockheed Martin – Dallas, Texas

Activity

- In May 2015 (Missile Flight Test 2) and November 2015 (Missile Flight Test 1), the Army conducted two live fire developmental tests in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) during which Northrup Grumman contractors used AIAMD to defeat missile threats. Both tests were conducted at White Sands Missile Range, New Mexico.

- In January 2016, the Army conducted a Cooperative Vulnerability and Penetration Assessment as part of a developmental test effort. The test was not conducted in accordance with a DOT&E-approved test plan. Results from this test will be incorporated in future software builds.
- From March through May 2016, the Army completed a LUT on AIAMD at White Sands Missile Range, New Mexico, and Fort Bliss, Texas. The LUT was conducted in accordance with a DOT&E-approved test plan. The LUT consisted of three phases:
  - Sustained operations phase (three 72-hour mission pulses)
  - Missile Flight Test 3-1 and 3-2
  - HWIL phase
- In July 2016, the Army conducted a developmental test of new IBCS software, version 3.2.1. Numerous system performance deficiencies were identified during Government Software Integration Laboratory assessments and soldier check-out events.

Assessment

- During the LUT, the operators' assessment was limited to basic air defense missions because of software immaturity and instability, as well as a lack of training for operators on new equipment and new capability operations. Due to AIAMD software immaturity and limited capability to effectively operate at a multi-echelon level, soldiers were unable to effectively coordinate with engagement and identification authorities, a key function in air defense.
- As of February 3, 2016, AIAMD's IBCS software had 32 Severity 1 and 2 software problem reports. Also, AIAMD demonstrated poor system reliability, with 6 to 8 hours of Mean Time Between System Abort (MTBSA) compared to the LUT entrance criteria of 31 hours MTBSA.
  - Despite DOT&E's concerns that AIAMD is an immature system and not ready for a Milestone C decision, the Army elected to proceed with the LUT as an operational test.
- During the LUT, AIAMD demonstrated a 6 percent likelihood that it could operate for 72 hours without experiencing a failure that would result in system abort.
  - The warfighter requirement is a 90 percent likelihood that the system will operate for 72 hours without experiencing a failure that results in system abort.
- The EOC, a critical subsystem of AIAMD, demonstrated an average operating time of up to 16 hours without a failure that results in ineffective operations; this is significant when compared to the minimum requirement to operate for up to 446 hours.
- The computer workstations in the EOC were not reliable and a constant source of frustration for operators.
  - Due to IBCS software immaturity, workstations lagged and froze during mission operations, significantly affecting crew operations and mission execution.
  - The median time to repair a workstation was approximately 13 minutes. During air defense operations against aircraft and missile threats, this could result in multiple failed engagements and loss of critical defended assets.
- During the majority of the sustained operations phase, the workstations showed multiple false tracks when only one test target aircraft was flying. The operators often struggled to identify targets of interest in the cluttered air picture.
- AIAMD was unable to effectively operate on the Link 16 network and had significant problems with dual tracks and reporting responsibility with the IBCS network. The LUT was the first time AIAMD attempted interoperability with the Marine Tactical Air Operations Center.
- The IFCN relays were not reliable. Additionally, on multiple occasions the IFCN relay was inoperable thus disconnecting the associated radar or shooter from the AIAMD system. Once the IFCN is disconnected, the operators are unable to employ that associated radar or shooter.
- The AIAMD system setup, operations, and maintenance technical manuals were incomplete or inadequate.
- In surveys, 40 percent of operators identified poor training (includes training time, documentation, and lesson plans) on system employment.
- In August 2016, Milestone C (planned for November 2016), was placed on hold until IBCS software deficiencies are resolved in accordance with contracted requirements. The Program Management Office is working with Northrop Grumman Corporation to resolve IBCS software deficiencies.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Fix all Severity 1 and 2 software problem reports and conduct another operational assessment of AIAMD performance to inform a Milestone C decision.
  2. Develop and publish an AIAMD operational mode summary/mission profile for planned AIAMD employment.
  3. Update the program TEMP in accordance with updated program acquisition way forward.
  4. Determine the required IBCS reliability for initial fielding and outline a reliability growth plan in an updated program TEMP.
  5. Correct and formalize all AIAMD system documentation and training deficiencies.

Chemical Demilitarization Program – Assembled Chemical Weapons Alternatives (CHEM DEMIL-ACWA)

Executive Summary

- Army testing of demilitarization systems in the Chemical Demilitarization Program has been adequate to ensure the safe and secure disposal of chemical warfare material.
- The Army conducted operational testing in accordance with DOT&E-approved test plans.
- The Army began operational testing at the Pueblo Chemical Agent-Destruction Pilot Plant (PCAPP) located in Colorado in FY16.
- Disposal operations of the U.S. chemical stockpile did not meet the original Chemical Weapons Treaty deadline of April 2007. Congress, through Public Law 114-38, has established a new stockpile elimination deadline of December 31, 2023.

System

- The Chemical Demilitarization Program involves the destruction of lethal chemical agents, chemical munitions, and non-stockpile chemical warfare material.
- The PCAPP stockpile disposal facility in Pueblo, Colorado, has started operations while the Blue Grass Chemical Agent-Destruction Pilot Plant (BGCAPP) facility in Richmond, Kentucky, is preparing for operations. These facilities employ chemical neutralization of agents followed by post-treatment of the neutralized products.
  - The PCAPP is a first-of-a-kind facility designed to destroy the chemical blister agent mustard (HD and HT) stored in 155 mm projectiles, 105 mm projectiles, and 4.2-inch mortar rounds through the use of a low-temperature, low-pressure neutralization process. PCAPP will process the neutralized agent (hydrolysate) using biotreatment.
  - The BGCAPP is a first-of-a-kind facility designed to destroy chemical nerve agents Sarin (GB) and VX stored in 155 mm projectiles, 8-inch projectiles, M55 rockets, and M56 rocket warheads through the use of a chemical (caustic) neutralization process. BGCAPP will process hydrolysate using supercritical water oxidation (SCWO) technology.
- Explosive destruction technology is used in the Assembled Chemical Weapons Alternatives (ACWA) program:
  - PCAPP uses the Explosive Destruction System (EDS) for destruction of problematic munitions not easily processed in the main plant. The EDS uses shaped explosive charges to access chemical munitions and destroy the munitions' explosive components. After detonation, EDS chemically treats the munitions' contents within the containment vessel and collects vapor and liquid samples as required. The products of this neutralization process (neutralents) are transferred to drums and will be packaged for shipment to an approved treatment, storage, and disposal facility (TSDF).
  - BGCAPP will use the Static Detonation Chamber (SDC) to destroy mustard munitions. The SDC uses explosive destruction technology designed to destroy conventional munitions, munition components, and chemical-filled munitions by indirect heating in a detonation chamber. The heat produced in the chamber allows for detonation and/or deflagration of the agent-filled munition and its energetic components, and subsequently treats the chemical fill. The air pollution abatement system captures and treats any resulting harmful vapor products.

Mission

The United States is using the Chemical Demilitarization Program to comply with the Chemical Weapons Convention. This is an arms control and nonproliferation treaty that requires the destruction of the U.S. stockpile of lethal chemical agents, chemical munitions, and chemical warfare material.

Major Contractors

- Chemical Materials Activity – Aberdeen, Maryland
- Assembled Chemical Weapons Alternatives (ACWA) sites:
  - Bechtel National, Inc. – San Francisco, California
  - Parsons Infrastructure and Technology Group, Inc. – Pasadena, California

Activity

- The Chemical Demilitarization Program is not a traditional acquisition program. DOT&E oversight began in 1999 when Congress directed that the DOD oversee this program as a major defense acquisition program due to cost and schedule overruns.

- The test and evaluation program for chemical demilitarization consists of two phases:
  - The developmental testing phase consists of system and subsystem component testing without an agent culminating in end-to-end operations of the facility.
  - The operational testing phase consists of pilot testing and campaign changeover testing involving operations with an agent. Operational testing supports a decision to proceed to full operational status for a specific agent/munitions campaign. For example, one campaign would destroy 155 mm projectiles containing mustard blister agent, another would destroy 8-inch projectiles equipped with Sarin nerve agent, and the third would destroy M55 rockets equipped with Sarin. After the completion of each campaign, the facility reverts to operational test status for changeover to the next planned campaign. This process is repeated until the destruction of all agent/munitions configurations in the site's stockpile is complete. DOT&E monitors the test activity and independently analyzes test data at PCAPP and BGCAPP.
- As of August 2016, the Chemical Demilitarization Program has destroyed over 90 percent of the total U.S. chemical weapons stockpile (originally 31,498 agent tons).
- On February 11, 2016, the PCAPP EDS completed the destruction of 560 overpacked munitions and agent containers that could not be processed by the main plant. The PCAPP EDS campaign began in March 2015 after successfully completing multiple pre-operational reviews.
- The systems contractor led by Bechtel successfully conducted an Integrated Operations Demonstration (IOD) in August 2016, demonstrating main plant facility readiness for operations.
- The Army conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA) on the industrial control system (ICS) and laboratory information system (LIS) at PCAPP. DOT&E observed all cybersecurity assessment activities. The Program Executive Office and the systems contractor committed to correcting defects prior to the start of operations, and the Army conducted two follow-on events to verify the correction of noted vulnerabilities.

Assessment

- Army testing of demilitarization systems in the Chemical Demilitarization Program has been adequate to ensure the safe and secure disposal of chemical warfare material. The U.S. Army Material Systems Analysis Activity (AMSAA) is providing effective independent oversight of the testing of both stockpile and non-stockpile programs. Fully integrated operational demonstrations that confirm all phases of operations (including preparation, destruction/neutralization, and disposal) remain critical prerequisites for transitioning to operations with live agents.
- Disposal operations of the U.S. chemical stockpile did not meet the original Chemical Weapons Treaty deadline of April 2007. Congress, through Public Law 114-38, has established a new stockpile elimination deadline of December 31, 2023.
- Cybersecurity testing at PCAPP identified technical and physical security vulnerabilities, which were corrected by the systems contractor and verified by both AMSAA and DOT&E.
  - Cybersecurity testing of the PCAPP LIS showed that the risk was low and acceptable based upon the assessment of the protect, detect, respond, and restore capabilities.
  - Cybersecurity testing of the PCAPP ICS resulted in a number of system improvements, including enhanced policies and procedures, installation of a Security Information and Event Management (SIEM) system for threat monitoring, and configuration of the SIEM to alert operators to suspicious activities. DOT&E and AMSAA have verified these improvements. The system contractor also made improvements to physical security following the AA.
  - The PCAPP IOD identified areas for procedural improvement, which were corrected and verified by the test community. The IOD demonstrated that the plant was ready to begin processing agent rounds as part of a controlled ramp-up (pilot testing). Following the correction of deficiencies noted during cybersecurity assessments and the IOD, PCAPP's main plant began processing chemical munitions as part of pilot (operational) testing on September 7, 2016. DOT&E is monitoring the pilot testing and operations.
- The BGCAPP test program started planning for FY17 activities by:
  - Developing IOD and pilot test plans for the SDC, to include a cybersecurity CVPA and AA. The SDC, based on current credible estimates, could begin processing mustard rounds in 4QFY17.
  - Planning cybersecurity test activities for the LIS, BGCAPP Main Plant, and SDC systems.
- AMSAA is monitoring BGCAPP systemization activities to support the readiness assessment to proceed into IOD.

Recommendations

- Status of Previous Recommendations. There are no outstanding previous recommendations.
- FY16 Recommendation.
  1. The Program Executive Officer ACWA should incorporate lessons learned from PCAPP test planning and cybersecurity testing at BGCAPP.

Command Web

Executive Summary

- Command Web is the Army's lead program to field a web-based set of tools designed in accordance with Common Operating Environment (COE) architectures and standards.
- During 2016, the Army conducted a two-phase Command Web Limited User Test (LUT) at Grafenwoehr, Germany, and Fort Bliss, Texas. The test was conducted in accordance with a DOT&E-approved test plan.
- The Army intends to use the results of the Command Web LUT to support a 3QFY17 material release decision.
- DOT&E's preliminary results for the Command Web LUT indicate:
  - Soldiers found Command Web tools easy to use and were successful at creating and posting engineer tasks on the Common Operational Picture (COP).
  - Since Command Web is a client-based application, the unit could install the tools on any computer within the command post. This allowed staff sections (beyond the intended engineer cell) to access the COP without the need of a legacy mission command hardware/software suite.
  - Lack of trained system administrators to manage tactical operations center (TOC) servers hinders Command Web's ability to support soldiers in the accomplishment of their mission. Training afforded soldiers did not allow them to troubleshoot server problems and share the COP between unit echelons and mission command applications.
  - Command Web demonstrated its reliability requirement.
- Command Web experienced cybersecurity vulnerabilities that could affect its ability to support the unit's mission.

1 - Soldier operating Command Web
2 - Command Post Computing Environment Map Widget
3 - Maneuver Widget

System

- Command Web is a collection of web-based applications or "widgets" designed to provide combat engineer staffs and leaders with tools that enhance tactical mission command at brigade and battalion command posts, and support their functional responsibility for the planning and execution of combat engineer tasks.
- The Army designed Command Web to fill an engineer capabilities gap created with the termination of the Maneuver Control System (MCS). Command Web provides web-based engineer tools to enhance the operations of Command Post of the Future (CPOF), which replaced MCS.
- Command Web includes the Obstacles and Hazards Services and Engineering Mobility Services widgets. These tools provide soldiers the ability to create, receive, and analyze obstacle and hazard information; road, route, and bridge information; and engineering project information.
- The Maneuver widget allows soldiers to view relevant COP information (e.g., maneuver graphics, friendly position location information, enemy situation) to provide context for executing combat engineer functions. The Maneuver widget supports collaboration with other engineer staff cells and with the integrated battle staff through the use of mission command applications during planning and execution phases of mission operations. Data and products from Command Web widgets are displayed on the Common Map widget.
- Command Web is the Army's lead program to field a web-based set of tools designed in accordance with COE architectures and standards. The Army intends for the Command Post Computing Environment V3.0 to provide these capabilities as part of a larger set of mission command tools and replace Command Web when fielded in FY19.

Mission

- Army combat engineer leaders and soldiers use Command Web tools to perform technical and operational tasks for mobility, counter-mobility, survivability, and construction to support the synchronization of engineer activities and their integration into maneuver operations.
- Engineer staff use Command Web widgets to synchronize engineer products via the COP, create and disseminate graphics, and publish/subscribe to data feeds from other Warfighter Functional Area mission command applications. Engineer soldiers and other Command Web users within the TOCs share and collaborate using a variety of data sources visualized on a common map. The Army intends Command Web products to inform commanders during the military decision-making process.

Major Contractor

- U.S. Army Communications – Electronics Command, Software Engineering Center, Aberdeen Proving Ground, Maryland

Activity

- During 2016, the Army conducted a two-phase Command Web LUT at Grafenwoehr, Germany, and Fort Bliss, Texas. The test was conducted in accordance with a DOT&E-approved test plan. The purpose of the Command Web LUT was to:
  - Assess Command Web effectiveness, suitability, and survivability, and provide an evaluation in support of the Army's planned 3QFY17 material release decision.
  - Assess Command Web's ability to fill the engineer capability gap created with the termination of MCS, and enhance the mission support provided by CPOF.
  - Assess Command Web's ability to support combat engineer functions at battalion and brigade, and update relevant engineer information to the unit's COP to share information across brigade mission command applications.
  - Provide performance insights and lessons learned for future testing and development of the Army's Command Post Computing Environment.
- The Army conducted the first phase of the Command Web LUT at Grafenwoehr, Germany, as part of a U.S. European Command joint coalition exercise during February 2016. The Germany test consisted of two assessment activities:
  - Soldiers and leaders from the 15th Engineer Battalion manned TOCs representing three battalions, a brigade, a division, and corps. The soldiers responded to operations orders and fragmentary orders to create combat engineer tasks in support of larger mission requirements using Command Web and mission command applications associated with their TOCs. The resulting products were posted to the COP and reviewed by subject matter experts for completeness and accuracy.
  - Soldiers and leaders from the 173rd Airborne Brigade Combat Team employed Command Web within the brigade's TOC in support of the unit's real-time training mission within the U.S. European Command joint coalition exercise. The unit integrated Command Web into their existing TOC servers, and distributed Command Web widgets to the brigade's combat engineer cell and other staff within the TOC. The brigade conducted noncombatant evacuation operations and used Command Web to produce engineer staff products in support of the unit's mission.
- The Army conducted the second phase of the Command Web LUT during the April through May 2016 Network Integration Evaluation (NIE) 16.2. The operational test employed the 2nd Brigade, 1st Armored Division conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. This phase of the test focused on unit's use of Command Web at brigade and battalion TOCs while performing operationally realistic missions supported by tactical communications.
- DOT&E approved a Command Web Test and Evaluation Master Plan update on July 21, 2016.

Assessment

- DOT&E and the Army are assessing Command Web LUT data to produce evaluations in support of the Army's 3QFY17 material release decision.
- DOT&E's preliminary results for the Command Web LUT indicate:
  - Soldiers found Command Web tools easy to use and were successful at creating and posting engineer tasks on the COP.
  - The airborne brigade commander was innovative in using Command Web by installing the tools in several staff sections within his TOC. Although Command Web was intended for the combat engineer cell, the unit could install the tools on any TOC computer since Command Web is a client-based application. This allowed staff sections to access the COP without the need of a legacy mission command hardware/software suite (e.g. CPOF).
  - Lack of trained system administrators to manage TOC servers hinders Command Web's ability to support soldiers in the accomplishment of their mission. During the Germany phase, system administrators were not able to troubleshoot server problems that slowed Command Web operations, and had to reboot the servers. During NIE16.2, system administrators were not able to configure TOC servers to share the COP with Command Web products between brigade and battalion, but could share the COP between Command Web and other mission command applications within their TOC.
  - Command Web demonstrated its reliability requirement during the Germany phase of test.
  - During NIE 16.2, Command Web experienced cybersecurity vulnerabilities that could affect its ability to support the unit's mission.

Recommendations

- Status of Previous Recommendations. This is the first annual report for Command Web.
- FY16 Recommendations. The Army should:
  1. Improve Command Web training to include system administrator training to install, operate, and maintain it, and integrate the unit's COP across mission command applications.
  2. Correct cybersecurity vulnerabilities and validate corrections during operational test.

Distributed Common Ground System – Army (DCGS-A)

Executive Summary

- DOT&E reported on January 29, 2016, that the Distributed Common Ground System – Army (DCGS-A) Increment 1, Release 2 is operationally effective and suitable, but not survivable against cyber threats due to the vulnerability of the Army network.
- The Defense Acquisition Executive approved the DCGS-A Increment 2 Material Development Decision on October 9, 2015.
- DCGS-A Increment 2 includes two releases. The Army Test and Evaluation Command (ATEC) will conduct the IOT&E with Release 1 in FY19 to inform the Full Deployment Decision in early FY20. The Army will continue Increment 2 development and testing with Release 2. The increment 2, Release 2 fielding decision is planned for FY22.

System

- DCGS-A is the Army Service component of the DOD DCGS family of systems, providing multi-Service integration of intelligence, surveillance, reconnaissance (ISR), and targeting capabilities. DCGS-A connects with the DCGS family of systems via the DCGS Integration Backbone (DIB). The DIB is a cohesive set of modular, standards-based data services focused on enterprise information sharing. The DCGS Multi-Service Execution Team manages the DIB.
- DCGS-A Increment 1, Release 2 is a command and control system that tasks, processes, exploits, and disseminates ISR information from battalion to Echelons Above Corps (EAC) by combining 16 independent legacy systems of record into one comprehensive network, including the capability to process Top Secret/Sensitive Compartmented Information.
- DCGS-A Increment 1 has a planned modernization strategy until Increment 2 fielding. The modernization efforts focus on end-of-life obsolescence and cyber updates. The system picture above shows the Increment 1, Release 2 configuration.
- DCGS-A Increment 2 will consist of a collection of software packages selected to provide each Army echelon from battalion to EAC the capability to synthesize and exploit intelligence data.
  - The software packages will be commercial off-the-shelf and government off-the-shelf hardware components, configured to meet the Army unit's intelligence mission and mobility requirements.
  - The program intends to deliver these Increment 2 capabilities in two releases. The Army will develop the Increment 2 configuration after the Milestone B decision in FY17.

Mission

- Army intelligence units use DCGS-A to fuse intelligence information and produce enemy situational awareness products.
- Army intelligence analysts use DCGS-A to perform receipt and processing of select ISR sensor data, intelligence synchronization, ISR planning, reconnaissance and surveillance integration, fusion of sensor information, and direction and distribution of relevant threat, non-aligned, friendly, and environmental (weather and geospatial) information.

Major Contractors

- General Dynamics – Taunton, Massachusetts
- ManTech – Fort Hood, Texas
- Booz Allen Hamilton – Aberdeen Proving Ground, Maryland
- Exelis Incorporation – Mclean, Virginia

Activity

- ATEC conducted the DCGS-A Increment 1, Release 2 FOT&E in May 2015 during the Army's Network Integration Evaluation (NIE) 15.2 at Fort Bliss, Texas, and in a database synchronization test at the Ground Station Integration Facility (GSIF) at Aberdeen Proving Ground, Maryland, in September 2015. Cybersecurity tests were conducted during NIE 15.2 and at the GSIF before and after the NIE 15.2. ATEC conducted the tests in accordance with the DOT&E-approved test plan, but did not conduct the data collection, reduction, and analysis as described in the test plan.

- DOT&E provided a report to Congress on January 29, 2016, evaluating DCGS-A based on data obtained from the test events.
- The Defense Acquisition Executive approved the DCGS-A Increment 2 Material Development Decision on October 9, 2015.
- DCGS-A Increment 2 includes two releases. ATEC will conduct the IOT&E with Release 1 in FY19 to inform the Full Deployment Decision in early FY20. The Army will continue Increment 2 development and testing with Release 2. The Increment 2, Release 2 fielding decision is planned for FY22.

Assessment

- DOT&E evaluated the Increment 1, Release 2 to be operationally effective and suitable, but not survivable against cyber threats due to the vulnerability of the Army network.
- DCGS-A Increment 1 is operationally effective. DCGS-A allows Army intelligence units to rapidly receive and organize intelligence from more than 700 sources, search relevant information, perform analysis, and share the results with the Army command and control network as well as the intelligence community through the DCGS Integration Backbone.
- DCGS-A Increment 1 is operationally suitable, provided the Army intensively trains DCGS-A users and provides continued refresher training to units in garrison. DCGS-A is a complex system, and the skills required to use it are perishable. The operational availability of DCGS-A satisfied the requirements at all echelons, and reliability improved from the IOT&E in 2012. There were no hardware failures during the FOT&E. Software failures were still a challenge for users; the system required reboots about every 20 hours for users who had heavy workloads such as the fire support analysts and data managers in Brigade Combat Team Tactical Operations Centers.
- The survivability results are classified but can be found in classified annex B of the January 2016 DOT&E report on DCGS-A Increment 1, Release 2 FOT&E.

Recommendations

- Status of Previous Recommendations. The Army is implementing the previously recommended actions.
- FY16 Recommendations.
  1. ATEC should continue to develop the Test and Evaluation Strategy for Increment 2.
  2. The Army should continue to provide intensive training to DCGS-A users, including refresher training to units in garrison.

HELLFIRE Romeo and Longbow

Executive Summary

- The HELLFIRE missile (AGM-114) is a family of air-to-surface, guided munitions consisting of a missile body with different warhead types. The Air Force authorized fielding of the latest HELLFIRE Romeo missile variant (with R warhead) in December 2014. Other Services have since pursued different variations of the HELLFIRE missile.
- The Army successfully completed testing of the Romeo missile in 2016 against a new, more representative masonry target at high temperature. The Army plans to implement the R warhead on the Joint Air-to-Ground Missile System, which begins developmental and live fire tests in FY17.
- The Navy plans to employ the HELLFIRE Longbow L8A variant, which utilizes the K2A warhead, on the Littoral Combat Ship (LCS) against threat boat swarms as part of the Surface-to-Surface Mission Module (SSMM). The Navy is in the process of crafting a developmental test program; the operational and live fire test programs were codified in change pages to the LCS Test and Evaluation Master Plan, which DOT&E approved in March 2016.
- The Navy began developmental HELLFIRE Longbow testing in FY15 with the Guided Test Vehicle – 1 (GTV-1) test. In December 2015 and August 2016, the Navy carried out GTV-2 developmental tests from a barge against small boat representative high-speed maneuvering surface targets. These tests could have been leveraged to support the DOT&E effectiveness/lethality evaluation but the Navy has planned and executed all GTV tests to date without DOT&E oversight.

System

- The AGM-114 HELLFIRE is a family of guided missiles for use against fixed and moving targets by both rotary- and fixed-wing aircraft, including unmanned aerial vehicles (UAVs).
- The HELLFIRE Romeo laser-guided missile variant:
  - Is an air-to-surface missile intended to be launched from Army and Air Force UAV platforms, Air Force Special Operations and Marine Corps fixed-wing aircraft (e.g., MC-130 and KC-130 variants), and Army rotary-wing aircraft. It uses a new warhead and a semi-active laser seeker to home in on its target.

  - Has a multi-function warhead that includes variable time delay fuzing options, in order to provide improved lethality against combatants within building structures while maintaining lethality against non-armored targets.
  - Is compatible with other HELLFIRE missiles fired from other Air Force UAVs.
- The HELLFIRE Longbow radar-guided missile variant:
  - Is being redesigned from its prior air-to-surface role as employed on Army Longbow Apache helicopters to a new role as a Navy surface-to-surface missile intended to be launched from LCS against threat boats in swarm attacks
  - Has a single-function K2A warhead with a fragmentation wrap designed to provide lethality against small boat targets

Mission

- Army, Air Force, and Marine Corps commanders will employ HELLFIRE Romeo from a range of UAV, fixed wing, and rotary wing platforms to engage enemy combatants located within complex building and bunker structures, in non-armored vehicles, in small boats, and in the open.
- Navy LCS commanders will employ HELLFIRE Longbow missiles as part of its SSMM against small threat boats involved in swarming attacks against the LCS.

Major Contractor

Lockheed Martin Corporation, Missiles and Fire Control Division – Grand Prairie, Texas
(The missiles are manufactured in Ocala, Florida, and Troy, Alabama.)

Activity

- In FY15, lot acceptance testing of HELLFIRE Romeo R warheads against non-operationally representative (harder than the requirement) masonry targets at elevated temperatures failed in two of the four tests. Subsequently, the Army tested the Romeo missile with the R warhead in June and August 2016 against the operationally representative target at high temperature. The warhead operated successfully in eight of eight tests.
- The Navy carried out GTV-2 HELLFIRE Longbow developmental tests against small boat representative high

speed maneuvering surface targets in December 2015 and August 2016 without DOT&E oversight. The Navy has not yet delivered an LFT&E Lethality Test Plan for the SSMM utilizing the HELLFIRE Longbow missile, which could have leveraged these developmental tests.

Assessment

- As reported in DOT&E reports to Congress in FY14, the HELLFIRE Romeo missile demonstrated adequate lethality across a spectrum of expected targets, including small boats, light armor, technical vehicles (trucks), and personnel both in the open and behind/under a variety of masonry structures.
- Army tests of the HELLFIRE Romeo R warhead, completed to support the testing and procurement of the Joint Air-to-Ground Missile program, verified the assessment of adequate lethality against the operationally representative masonry target but have not addressed the underlying cause of the observed failures against harder targets.
- The Navy conducted the early developmental tests of the HELLFIRE Longbow without DOT&E involvement or oversight, missing an opportunity to leverage these data in operational effectiveness and lethality assessments.

Recommendations

- Status of Previous Recommendations. The Army has begun to address the recommendations in the 2015 DOT&E classified report to further quantify lethality estimates against specific targets in specific conditions and engagement circumstances. However, several target types require additional characterization. The Air Force provided the classified test results to the Joint Technical Coordinating Committee for Munitions Effectiveness (JTCG/ME) for incorporation into JTCG/ME products as indicated in the final classified DOT&E report.
- FY16 Recommendations.
  1. The Army HELLFIRE program should characterize the spectrum of masonry target conditions (hardness, density, etc.) where the Romeo warhead fails to detonate when operating at high temperature.
  2. The Navy should develop a Lethality Test Plan for the SSMM utilizing the HELLFIRE Longbow missile, which must be approved by DOT&E.
  3. The Navy should fully fund and fully execute the operational and live fire test plans articulated in the 2016 update to the LCS Test and Evaluation Master Plan.

Javelin Close Combat Missile System – Medium

Executive Summary

- In FY16, the Army tested the Spiral 2 missile improvements and continued development of Spiral 3 missile improvements and a new Light Weight Command Launch Unit (CLU). The Army intends these efforts to improve lethality against non-armored targets and to reduce unit cost and weight.
- Early arena testing and lethality modeling of the Spiral 2 missile, which includes a new Multi-Purpose Warhead (MPWH), has demonstrated improved warhead fragmentation and similar armor penetration compared to the legacy warhead. This indicates the potential for improved lethality against non-armored targets and personnel in the open while maintaining performance against armored threats.
- The precursor warhead (PCWH) has failed to detonate in two of two flight tests and two of nine static warhead tests, and the MPWH failed to detonate in one of nine static warhead tests. The Army stopped the testing of the Spiral 2 missile and convened a failure review board to investigate the cause of the failures. Testing of the Spiral 2 missile will continue into FY17 following resolution of the warhead detonation problems.
- The Program Office has chosen to delay production of the FGM-148F or Spiral 2 missile until the successful resolution of the warhead failures and completion of the missile test program in FY17.
- DOT&E and the Army are planning testing required for the Spiral 3 missile and Light Weight CLU developments.

System

- The Javelin Close Combat Missile System – Medium is a man-portable, fire-and-forget, anti-tank guided missile employed by dismounted troops to defeat threat armored combat vehicles out to 2,500 meters.
- The Javelin system consists of a missile in a disposable launch tube assembly and a re-usable CLU. The CLU mechanically engages the launch tube assembly for shoulder firing, has day and night sights for surveillance and target acquisition, and electronically interfaces with the missile for target lock-on and missile launch. An operationally-ready Javelin system weighs 49.5 pounds.
- The Javelin missile employs a tandem shaped charged warhead to defeat vehicle armor and can be fired in direct-fire or lofted trajectory top-attack modes.
- The Army has planned four Javelin system improvements to reduce unit cost and weight and improve lethality against non-armored targets. These improvements are referred to as missile Spiral 1, 2, 3, and Light Weight CLU.
  - The Spiral 1 effort will replace electronic components in the control actuator section of the missile for cost and weight savings. Production missiles will be designated FGM-148E.
  - The Spiral 2 effort will develop an MPWH, which uses enhanced fragmentation to improve lethality against non-armored targets and personnel in the open while maintaining lethality against armored threats. Production missiles will be designated FGM-148F.
  - The Spiral 3 effort will develop a new launch tube assembly and battery unit, and will replace the current gas-cooled seeker with an uncooled seeker in the guidance section of the missile. Production missiles will be designated FGM-148G.
  - The Light Weight CLU effort will develop a new CLU that is smaller and lighter while maintaining or improving system performance.

Mission

- Infantry, Engineer, Reconnaissance, and Special Operations Forces within Army and Marine Corps ground maneuver units employ the Javelin to destroy, capture, or repel enemy assault through maneuver and firepower.
- Service members use the Javelin to destroy threat armor targets and light-skinned vehicles, and to incapacitate or kill threat personnel within fortified positions. In recent conflicts, Javelin was used primarily against enemy bunkers, caves, urban structures, mortar positions, snipers, and personnel emplacing IEDs.

Major Contractors

- Raytheon – Tucson, Arizona
- Lockheed Martin – Orlando, Florida

Activity

- In 2016, the Army Aviation and Missile Research, Development, and Engineering Center continued testing of the Spiral 2 missile improvements in accordance with the DOT&E-approved live fire strategy. A total of 7 of 21 planned missile flight tests and 9 of 16 planned static warhead tests have been conducted at the Redstone Test Center, Alabama.
  - Of the seven flight test missiles, one was a tactical round including both a PCWH and MPWH, one contained a PCWH and telemetry payload, and five contained a telemetry payload only
  - The nine static tandem warhead tests included both the PCWH and MPWH
- DOT&E and the Army are planning testing required for the Spiral 3 missile and Light Weight CLU.
- The Javelin Program Office completed testing of the Spiral 1 missile improvements and approved the FGM 148E for the FY17 production lot.

Assessment

- Missile Warhead Performance:
  - Preliminary results of static warhead testing of the MPWH indicate improved fragmentation versus the legacy warhead while maintaining effectiveness against armor. The Army intends the improved fragmentation to enhance lethality of the weapon against non-armored targets and personnel in the open.
  - The PCWH failed to detonate in two of nine static tests and in two of two flight tests. The MPWH failed to detonate in one of nine static tests. Prior Government qualification testing at a contractor facility demonstrated no PCWH or MPWH failures in 62 static tandem warhead tests.
  - The Army conducted investigations after the first two PCWH and the one MPWH failures. Potential problems with the static test setup at Redstone Test Center were corrected and testing resumed. The Army stopped testing and initiated a failure review board after two more PCWH failures occurred. Testing of the Spiral 2 missile will continue following identification and resolution of the failures.
- Missile Flight and Tracking Performance:
  - In seven of seven flight tests conducted to date, the Spiral 2 missiles have demonstrated proper target lock on and missile launch resulting in six successful hits and one miss. The six successful hits were against five tank targets and one pickup truck target; the miss was against a three-man IED team in the open. The miss is attributed to a combination of test range conditions that pulled the tracker off of the target during the flight. Personnel in the open are a secondary target for the Javelin.
- The Program Office has chosen to delay production of the FGM-148F, Spiral 2 missile, until the successful resolution of the warhead failures and completion of the missile test program in FY17.

Recommendations

- Status of Previous Recommendations. The Army and DOT&E are planning testing required for the Spiral 3 and Light Weight CLU. The Army agrees that an operational test should be conducted prior to fielding to confirm that effectiveness/lethality and suitability have not been compromised, and to ensure compatibility with applicable fielded variants of the missile.
- FY16 Recommendation.
  1. The Javelin Program Office should update the Javelin Test and Evaluation Master Plan in preparation for Spiral 3 and Light Weight CLU testing.

Joint Light Tactical Vehicle (JLTV) Family of Vehicles (FoV)

Executive Summary

- The industry protest after the Army awarded the Joint Light Tactical Vehicle (JLTV) initial production contract delayed the program schedule by 6 months. The Multi-Service Operational Test and Evaluation (MOT&E) is planned for February 2018. The Army and Marine Corps Initial Operational Capability dates are scheduled for 1QFY20.
- In May 2016, the Defense Acquisition Executive delegated the Milestone Decision Authority for JLTV to the Army, designating the program Acquisition Category 1C.
- In July 2016, DOT&E approved the JLTV Milestone C Test and Evaluation Master Plan (TEMP). The TEMP approval was delayed by 10 months based on the Army decision to submit the TEMP after the JLTV low-rate initial production contract award and review of the test program budget. The Army's intent was to reduce test costs based on assessing the extent of JLTV production design changes relative to the JLTV prototype vehicles performance during Engineering Manufacture Development (EMD) testing.
- Based on the JLTV Allocation Baseline Review, the program plans to implement several design changes intended to improve JLTV performance:
  - A new piston pump that reduces suspension transition times and increases reliability
  - Larger ammunition storage racks
  - Smaller engine air filter mount to improve driver visibility
  - Replacing several aluminum parts with steel to improve reliability
  - Replacing composite armors with all-metal to eliminate the multi-hit problem with ceramic armors
  - Modified gunner restraint system to improve gunner protection during underbody blast events
- The program plans to replace:
  - The engine used in the prototype JLTVs during EMD, with a newer model. The new engine will require several design modifications to fit in the engine compartment.
  - The roof hatch on the General Purpose and Utility variants with a bolt-on cover plate that eliminates a crew egress point.

System

- The JLTV Family of Vehicles (FoV) is the Marine Corps and Army partial replacement for the High Mobility Multi-purpose Wheeled Vehicle (HMMWV) fleet. The Services intend JLTV to provide increased crew protection against IEDs and underbody attacks, improved mobility, and higher reliability than the HMMWV.

General Purpose

Heavy Guns Carrier

Utility/Shelter Carrier

Close Combat Weapons Carrier

- The JLTV FoV consists of two vehicle categories: the JLTV Combat Tactical Vehicle, designed to seat four passengers, and the JLTV Combat Support Vehicle, designed to seat two passengers.
- The JLTV Combat Tactical Vehicle has a 3,500-pound payload and three mission package configurations:
  - Close Combat Weapons Carrier Vehicle
  - General Purpose Vehicle
  - Heavy Guns Carrier Vehicle
- The JLTV Combat Support Vehicle has a 5,100-pound payload and one mission package configuration:
  - Utility Prime Mover that can accept a shelter
- JLTVs are equipped with two separate armor levels: the A-kit, or base vehicle, which is intended for use in low-threat environments, and the B-kit, an add-on armor kit, for additional force protection to include enhanced small arms, fragmentation, and underbody protection in the intended deployment configuration.

Mission

- Commanders employ military units equipped with JLTV as a light, tactical-wheeled vehicle to support all types of military operations. JLTVs are used by airborne, air assault, amphibious, light, Stryker, and heavy forces as reconnaissance, maneuver, and maneuver sustainment platforms.
- Small ground combat units will employ JLTV in combat patrols, raids, long-range reconnaissance, and convoy escort.

Major Contractor

Oshkosh Corporation – Oshkosh, Wisconsin

Activity

- The industry protest after the Army awarded the contract delayed the program schedule by 6 months. The MOT&E is planned for February 2018. The Army and Marine Corps Initial Operational Capability dates are scheduled for 1QFY20.
- The program conducted a JLTV Allocation Baseline Review in February 2016. The meeting covered details of the JLTV design changes, vendor's organization, and manufacturing processes to improve vehicle performance, simplify production, and reduce cost.
- In May 2016, the Defense Acquisition Executive delegated the Milestone Decision Authority for JLTV to the Army, designating the program Acquisition Category 1C.
- In July 2016, DOT&E approved the JLTV Milestone C TEMP. The Army/Marine Corps TEMP submission to OSD was delayed by 10 months based on the Army/Marine Corps decision to submit the TEMP after the JLTV low-rate initial production contract award. The goal was to reduce the test budget based on assessing the extent of JLTV production design changes relative to JLTV prototype vehicles performance during EMD.
- The program began armor coupon live fire testing in July 2016 and ballistic cab testing in August 2016.
- The Army received the first delivery of production JLTVs in October 2016. The initial order included 657 JLTVs and 25 trailers.
- The Army Test and Evaluation Command (ATEC) began Reliability Qualification Testing (RQT) in January 2017 at Aberdeen Test Center, Maryland, and Yuma Proving Ground, Arizona. The objective of the RQT is to assess whether the JLTV can meet the Mean Miles Between Operational Mission Failure requirement prior to MOT&E. This testing is planned to consist of 96,000 miles on JLTVs.
- Full-Up System-Level live fire testing, intended to evaluate crew survivability and vehicle performance against mine and IED threats, overhead artillery, rocket-propelled grenades, homemade explosives, and the performance of the Automatic Fire Extinguishing System, is scheduled to begin in January 2017 at Aberdeen Test Center.
- The ATEC plans to conduct extreme cold weather testing beginning in February 2017 at Cold Regions Test Center in Fort Greeley, Alaska. The testing will provide information to assess the JLTV performance and reliability in extreme cold weather environments.

Assessment

- In August 2015, DOT&E's JLTV Milestone C Operational Assessment and classified Live Fire Report recommended the program develop a plan to improve the performance of the JLTV:
  - Increase the speed of suspension and tire pressure adjustments to improve vehicle responsiveness and maneuver
  - Strengthen the vehicle hood and add steps and hand-holds on the side of the vehicle to support rigging/de-rigging, ingress/egress, weapon mounting, and loading task
  - Redesign the JLTV to allow access to the cargo compartment from within the cab
  - Relocate mission equipment to improve storage of additional ammunition in the cab, and redesign ammunition platforms and storage straps in the cab to better accommodate ammunition cans
  - Reduce the Essential Function Failure rate, focusing on the sub-systems with high-failure rate
  - Fix command and control failures
  - Mitigate effect of placing items under energy absorbing seats to improve occupant protection
  - Improve gunner protection during underbody blast events
  - Modify frame clip systems to improve recoverability
  - Modify cooling lines to prevent coolant intrusion into crew cab
- Based on the JLTV Allocation Baseline Review, the program intends to implement several design changes to improve JLTV performance:
  - A new piston pump that reduces suspension transition times and increases reliability
  - Larger ammunition storage racks
  - Smaller engine air filter mount that improves driver visibility
  - Replacing several aluminum parts with steel to improve reliability
  - Replacing composite armors with all-metal to eliminate multi-hit problem with ceramic armors
  - Modified gunner restraint system to improve gunner protection during underbody events
- The program is developing and prioritizing the following Engineering Change Proposals:
  - Integration of a weight-bearing hood
  - Investigate modifying the Utility variant to support carrying troops in the rear cargo bed
  - Redesign the JLTV to fit a litter in the JLTVs
- Replacing aluminum parts with cast iron parts and ceramic armor with metal is intended to improve the multi-hit protection capability but will increase the JLTV weight by approximately 250 pounds.
- The engine used in the prototype JLTVs during EMD is being replaced by a newer model. The new engine will require several design modifications to fit within the JLTV engine compartment.

Recommendations

- Status of Previous Recommendations. The Army has made progress addressing the previous FY15 recommendations.
- FY16 Recommendations. None.

Joint Tactical Networks (JTN)
Joint Enterprise Network Manager (JENM)

Executive Summary

- DOT&E assessed the Joint Enterprise Network Manager (JENM) during the Mid-tier Networking Vehicular Radio (MNVR) Limited User Test (LUT) during the Network Integration Evaluation (NIE) 15.2.
  - Contractors using JENM were able to plan, configure, and load MNVRs prior to the LUT. Soldiers did not demonstrate these tasks during the operational test.
  - Soldiers were trained on JENM, but they could not effectively monitor or manage MNVR networks, or characterize the health of individual MNVR nodes and Wideband Networking Waveform (WNW) links.
- The Army's development, test, and fielding strategy since moving into sustainment has been to conduct government testing of JENM with waveforms, perform operational assessments based on surveys, and field new software increments. Project Manager (PM) Warfighter Information Network – Tactical (WIN-T) is developing a Test and Evaluation Master Plan (TEMP) that describes the test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- The Army collected data from the Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation 2 (MOT&E 2), NIE 16.2, Army Warfighting Assessment 17.1, and WNW simulation testing at the program manager's San Diego, California, facility to support a fielding of JENM 3.3. Data to support the fielding consisted of developmental testing and operator interviews and surveys.

System

- JENM is the Army enterprise solution for network operations to the Joint Tactical Network (JTN). JENM is designed to support planning, loading, monitoring, and managing current and future waveforms and software-defined radios.
- Software-defined waveforms are loaded into and considered a part of a radio set. JENM is capable of supporting radios integrated with the following software-defined waveforms: Soldier Radio Waveform (SRW), WNW, Single Channel Ground and Airborne Radio System (SINCGARS), ultra-high frequency satellite communications (SATCOM), and MUOS.

- The Army intends JENM to:
  - Provide network operations to current and future waveforms and software-defined radios. Current software-defined radios include Rifleman Radio, Manpack Radio, and MNVR. JENM will support the future Airborne Maritime Fixed Station Small Airborne Networking Radio.
  - Enable configuration, loading, monitoring, and management of the tactical radio network.
  - Provide an enterprise over-the-air management (eOTAM) capability. eOTAM is a real time command/response protocol between JENM and radios, enabling over-the-air radio and network management with JENM as the controller.

Mission

- Military forces use the software-defined radios to communicate and create networks to exchange voice, video, and data during all aspects of tactical military operations.
- Signal staffs use JENM to:
  - Plan, load, monitor, configure, troubleshoot, and prioritize network operations involving software-defined radio sets running SRW, WNW, SINCGARS, and tactical SATCOM
  - Provision a MUOS terminal to connect to a MUOS satellite network

Major Contractor

Government-developed by Network Management Reference Implementation Laboratory – San Diego, California

Activity

- As previously reported in the FY15 Annual Report (MNVR article), DOT&E assessed JENM 3.1 as a part of the MNVR LUT during NIE 15.2. The Army conducted the test according to a DOT&E-approved test plan. Prior to the LUT, contractors planned and configured the WNW and SRW networks. Contractors loaded the network plan and communications security (COMSEC) into the MNVR radios. During the exercise, soldiers attempted to monitor and manage the network.

- Although still funded as one program, the JTN program split responsibilities for JENM and Waveforms between two PMs. Responsibility for JENM transferred from PM JTN to PM WIN-T. PM Tactical Radios assumed responsibility for the waveforms.
- JENM had a draft TEMP prior to the transition from PM JTN to PM WIN-T. PM WIN-T is developing a TEMP that describes the test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- Consistent with the previous test and evaluation strategy, the Army collected data to support the fielding of JENM 3.3 consisting of developmental testing and operator interviews and surveys. The Army collected data during MUOS MOT&E 2, NIE 16.2, Army Warfighting Assessment 17.1, and government-conducted WNW simulation testing.
  - In October 2015, during MUOS MOT&E 2, soldiers equipped with JENM 3.2 provisioned Manpack radios using the Simple Key Loader to load COMSEC keys and MUOS terminal profile information.
  - Prior to NIE 16.2, the Army conducted new equipment training for soldiers on how to configure a network with JENM 3.3. During the validation exercise, soldiers loaded network plans and COMSEC keys on Manpack radios running SRW, SATCOM, and SINCGARS waveforms. The Army assessed the ability of the unit equipped with JENM to execute network management and monitoring tasks.
  - During NIE 16.2, contractors demonstrated some eOTAM functionality with Manpack and MNVR over the SRW and WNW networks as a proof of concept.
  - During Army Warfighting Assessment 17.1, the Army conducted an over-the-shoulder assessment of soldiers configuring, loading, monitoring, and managing a WNW network on the MNVR with JENM 3.3.

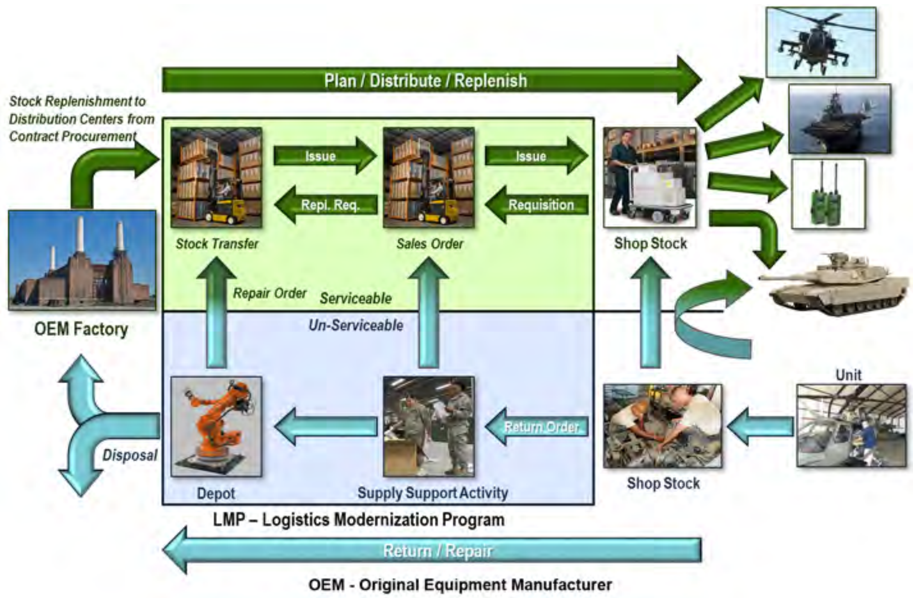
Assessment

- During the MNVR LUT at NIE 15.2, soldiers could not effectively monitor or manage MNVR networks with JENM 3.1, and were not able to characterize the health of individual MNVR nodes or individual WNW links. Contractors using the JENM were able to plan, configure, and load MNVRs prior to the LUT.
- In October 2015 during MUOS MOT&E 2, soldiers took several days to provision the Manpacks and they relied on contractors to complete the loading and provisioning of the radios.
- During the NIE 16.2 validation exercise, soldiers loaded network plans and COMSEC on Manpack radios running SRW, SATCOM, and SINCGARS waveforms. Soldiers were comfortable with the loading process. It took between 1.5 to 2.0 hours to load all of the radios in a company. The Army observed the ability of the unit equipped with JENM to execute network management and monitoring tasks. At the company level, communications soldiers are too busy to monitor the SRW network. JENM network monitoring of SRW lacks a map display showing the location of the radios.
- During Army Warfighting Assessment 17.1, the loading of the radio-configuration files and COMSEC keys was complicated and lengthy. Soldiers used JENM to configure the WNW network over-the-air by conducting over-the-air zeroization with the support of contractors.
- The PM demonstrated JENM's capability to monitor the WNW network and conduct eOTAM at a laboratory event using WNW simulation.
- The Army's development, test, and fielding strategy since moving into sustainment has been to conduct government testing of JENM with waveform versions, perform operational assessments based on surveys, and field new software increments.
  - The JENM program in the past 18 months has coordinated its schedule with Waveforms and not Tactical Radio programs. This process has precluded the ability to discover radio-unique integration problems. The implementation of waveform protocols is unique to each vendor. In addition, waveforms are frequently updated, so the version on the tactical radio available at operational testing may not be the version the JENM product office has built to. Changing focus of coordination to the Tactical Radio programs would synchronize JENM with both the radios and the waveform resident on the radio for both testing and fielding.
  - The operational evaluation strategy, based on surveys and observations, lacks an objective assessment of the effectiveness of the system. Future evaluations require instrumented data to verify JENM capabilities.
  - To remedy this, PM WIN-T is developing a TEMP that describes an adequate test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- The Army tactical network is complex for soldiers to design and plan. Network planning consists of developing the signal support architecture and radio platform preset architecture (Internet Protocol addressing and router programming). In all cases this is done by government engineers and contractors. Soldiers have executed network configuration (i.e., establishing call groups) with significant training, retraining, and contractor assistance.
- JENM has improved in usability and functionality with each software version as indicated by the ability of the soldiers to successfully perform network loading tasks without contractor assistance with JENM 3.3. Future capabilities and upgrades should be undertaken against prioritized and validated requirements.

Recommendations

- Status of Previous Recommendations. The Army still needs to evaluate the force structure requirements of adding software-defined, networking radios and network management responsibilities into company-level organizations.
- FY16 Recommendations. The Army should:
  1. Complete a JENM TEMP that describes robust testing and objective evaluations of the JENM in conjunction with the Army's software-defined radio operational tests.
  2. Prioritize and validate the requirements for JENM.
  3. Reduce the need for contractors and reduce the complexity of soldier tasks for network configuration.

Logistics Modernization Program (LMP)



Executive Summary

- From September 8 through November 20, 2015, the Army Test and Evaluation Command (ATEC) conducted the IOT&E of the Logistics Modernization Program (LMP) Increment 2 Wave 3 Release 7 at three Army Materiel Command (AMC) depots. The test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- LMP is operationally effective. The system successfully completed 98 percent of the observed tasks and successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems in 2015. Since LMP Increment 2 Wave 3 Release 7 went live in June 2015, users reported zero critical or major problems.
- LMP is operationally suitable; however, usability and user workload need improvement. LMP performance exceeded the requirements for system reliability and availability.
- LMP is survivable against an unaided outsider cyber threat having nascent- to limited-level capabilities, but demonstrated it is vulnerable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity Verification of Fixes (VoF), LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing.
- In support of its 2015 Cyber Economic Vulnerability Assessment (CEVA), the LMP Program Management Office (PMO) chose a commercial vendor that had provided cybersecurity economic subject matter expertise on another Enterprise Resource Planning (ERP) program; however, the vendor's lack of experience regarding LMP and AMC's business processes yielded only high-level findings and recommendations.
- On September 2, 2016, AMC made a full deployment declaration for LMP Increment 2, which will allow the increment to transition to the operation and sustainment phase of the acquisition lifecycle.

System

- LMP is the Army's core logistics Information Technology initiative and is one of the world's largest, fully integrated supply chain, maintenance, repair and overhaul, planning, execution, and financial management systems.
- LMP is an SAP-based commercial off-the-shelf ERP solution that manages and tracks orders and delivery of materiel from the AMC to soldiers where and when they need it.
- LMP transforms Army logistics operations in eight core business areas: acquisition, distribution, finance, product lifecycle management, supply chain planning, depots/arsenals (formerly manufacturing/remanufacturing), maintenance, and warehouse inventory management.
- LMP replaced the two largest national-level logistics systems: the inventory management Commodity Command Standard System, and the depot and arsenal operations Standard Depot System. LMP Increment 2 expands on the already deployed/operational production baseline to specifically address shop floor automation, automatic identification technology, and expanded ammunition requirements. Increment 2 improves outdated or manual processes, updates the other Army ERP systems with relevant information about the Army's military equipment, and provides the tools to support total asset visibility.
- LMP is currently deployed to approximately 30,000 users in more than 50 Army and DOD locations around the world, and interfaces with more than 80 DOD systems.

Mission

The AMC uses LMP to sustain, monitor, measure, and improve the Army's modernized national-level logistics support in order to save Army manpower and money through streamlined activities and greater visibility of logistics operations.

Major Contractors
- CSRA – Fairfax, Virginia
- INSAP Services Inc. – Marlton, New Jersey
- Attain, LLC – McLean, Virginia

Activity
- From September 8 through November 20, 2015, ATEC conducted an adequate IOT&E of the LMP Increment 2 Wave 3 Release 7 at three AMC depots (Corpus Christi Army Depot, Texas; McAlester Army Ammunition Plant, Oklahoma; and Rock Island Arsenal, Illinois). The Army conducted all testing in accordance with a DOT&E-approved test plan.
- Army Research Laboratory's Survivability/Lethality Analysis Directorate conducted a cybersecurity VoF January 19 – 22, 2016, and a follow-up cybersecurity VoF August 1 – 4, 2016.
- On September 2, 2016, the AMC signed a full deployment declaration memorandum for LMP Increment 2, which ends the technical and testing requirements allowing the increment to transition to the operation and sustainment phase of the acquisition lifecycle. DOT&E will continue oversight of LMP's improvements to cybersecurity.
- In FY17, LMP is scheduled to transition its program and data to Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs).

Assessment
- LMP is operationally effective.
  - During the IOT&E, users successfully completed 98 percent of the observed Mission Critical Function (MCF)-associated tasks and the Business Operations Test (BOT) confirmed that all but one of the remaining tasks functioned correctly.
  - LMP had no Severity 1 "critical" or Severity 2 "major" problems since the system went live in June 2015. LMP successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems during 2015.
  - Data collectors did not observe some tasks during the IOT&E because the test took place at live, operational locations and users did not perform the tasks over the course of the IOT&E. Data associated with Item Unique Identification (IUID) were not collected because IUID tags have not been placed on all Army logistics items.
  - ATEC assessed LMP Increment 2 as not effective because testers observed only 67 percent of the MCFs during the IOT&E. DOT&E disagrees with the ATEC assessment because testers observed all the missing MCF tasks during the BOT. The BOT involved actual LMP operators using realistic LMP data on a production-representative system.
- LMP is operationally suitable. Users surveyed during the IOT&E rated LMP a mean System Usability Scale score that is representative of "ok" usability and noted their workload remains high because they are using legacy systems concurrently with LMP. This will be the case until LMP completely replaces legacy systems in FY18. LMP demonstrated a Mean Time Between System Failure (MTBSF) of 1,026 hours, which exceeded the requirement of 110 hours MTBSF. LMP had an availability of 96 percent meeting the 95 percent requirement.
- LMP is survivable to an unaided outsider cybersecurity threat having nascent- to limited-level capabilities, but is not survivable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity VoF, LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing. The remaining low-risk vulnerabilities are either mitigated or will be corrected after LMP migrates to DISA DECCs.
- The 2015 CEVA portion of the LMP cybersecurity testing was inadequate because the LMP PMO chose a commercial vendor that lacked experience with LMP and AMC's business processes and because the vendor failed to conduct a significant portion of the CEVA. Although the vendor had provided cybersecurity economic subject matter expertise on another ERP program, its work during the LMP CEVA yielded only high-level findings and recommendations.
- Although the CEVA was inadequate, the overall test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- During its annual continuity of operations (COOP) test in December 2015, LMP demonstrated the feasibility of, but did not conduct, a transfer of operations to and from the COOP location.
- The 2010 National Defense Authorization Act requires financial audibility by 2017. The Program Office continues to work to achieve certification in accordance with the Federal Financial Management Improvement Act through various audits.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The LMP Program Office should:
  1. Conduct an FOT&E of LMP, focused on IUID and the tasks that were not observed during the IOT&E, when the IUID capability is fully available to LMP users.

2. Continue to survey LMP users to determine if the problem of increased user workload relative to legacy systems is improving.
3. After LMP data and program services transition to DISA DECCs, conduct another cybersecurity test from both the insider and outsider posture to verify the correction of known vulnerabilities and to possibly identify new vulnerabilities.
4. Ensure the cybersecurity economic subject matter experts chosen for the next CEVA understand the operational capabilities and key business processes used within the system to include roles and responsibilities.
5. Use the transition to the DISA DECCs to simulate a full transfer of operations to and from the COOP location.

M109A7 Family of Vehicles (FoV) Paladin Integrated Management (PIM)

Executive Summary

- The Army continued multiple phases of the M109 Family of Vehicles (FoV) Paladin Integrated Management (PIM) developmental testing at Yuma Proving Ground, Arizona, that included live firing performance, automotive performance, and reliability.
- The Army continued with live fire testing of the underbody IED protection kit, validation live fire testing of modified armored areas, and simulated damage testing of the electrical system at Aberdeen Proving Ground, Maryland.
- The Army began the M109 FoV PIM IOT&E in October 2016 at Fort Hood, Texas, but suspended it due to safety concerns. DOT&E will submit an IOT&E report in 2QFY17. A second IOT&E will be rescheduled for FY18 once corrective actions are complete.

System

- The M109 FoV PIM consists of two vehicles: the Self-Propelled Howitzer (SPH) and Carrier Ammunition Tracked (CAT) resupply vehicle.
  - The M109A7 SPH is a tracked, self-propelled 155 mm howitzer designed to improve sustainability over the legacy M109A6 howitzer fleet. The production howitzers have a modified M109A6 turret with a high-voltage electrical system and a modified Bradley Fighting Vehicle chassis, power train, and suspension. The M109A7 does not include upgrades to the cannon. A crew of four soldiers operates the SPH and can use it to engage targets at ranges of 22 km using standard projectiles and 30 km using rocket-assisted projectiles.
  - The M992A3 CAT supplies the SPH with ammunition. The full-rate production ammunition carriers have a chassis similar to the SPH. The ammunition carriers are designed to carry 12,000 pounds or 98 rounds of ammunition in various configurations. A crew of four soldiers operates the CAT.
- The Army will equip the SPH and CAT with two armor configurations to meet two threshold requirements for force protection and survivability – Threshold 1 (T1) and Threshold 2 (T2).
  - The base T1 armor configuration is integral to the SPH and CAT. The Army intends the T2 configuration to meet protection requirements beyond the T1 threshold with add-on armor kits.
  - The Army plans to employ PIM vehicles in the T1 configuration during normal operations and will equip the SPH and CAT with T2 add-on armor kits during combat operations.
- The Army designed an underbody kit to determine the potential protection an SPH and CAT could provide against IEDs similar to those encountered in Iraq and Afghanistan. The Army purchased five underbelly kits for test purposes. At this time, the Army does not intend to equip the SPH or CAT with the underbody kit.
- The Army intends to employ the M109 FoV as part of a Fires Battalion in the Armored Brigade Combat Team and Artillery Fires Brigades to support any Brigade Combat Team.
- The Army plans to field up to 557 sets of the M109 FoV with full-rate production planned for FY17.

Mission

Commanders employ field artillery units equipped with the M109 FoV to destroy, defeat, or disrupt the enemy by providing integrated, massed, and precision indirect fire effects in support of maneuver units conducting unified land operations.

Major Contractor

BAE Systems – York, Pennsylvania

Activity

- In FY16, the Army received 16 low-rate initial production (LRIP) SPH and CAT vehicles and conducted Production Qualification Testing (PQT) on the CAT and SPH at Yuma Proving Ground, Arizona:
  - PQT of LRIP vehicles included Cold Regions testing, performance live firing and automotive testing, characterization testing with T2 armor and underbelly kit, testing with the Crew Remote Operated Weapon System, and the Logistics Demonstration to validate operator and maintainer technical manuals and work packages.
  - The program began replacement of the steel cannon tubes with chrome-lined tubes to address tube wear and corrosion issues caused by use of the Modular Artillery Charge System (MACS).
  - In concert with the Program Executive Office Ammunition, the PIM program will use a redesigned M82 primer in IOT&E to better withstand pressures introduced by the higher zones (4&5) of the MACS propellant charges.
- The Army continued the execution of the LFT&E program at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans:
  - Exploitation testing on the CAT to validate armor modifications. Additional exploitation testing will be conducted on the SPH to complete validation of modifications to the T1 and T2 armor systems, made to address vulnerable areas identified in early testing.
  - Controlled damage experimentation on the high voltage electrical system to determine the consequences of ballistic damage.
  - The Army conducted all LFT&E in accordance with DOT&E-approved test plans.
  - The Army began full-up system-level testing of the M109 SPH and CAT resupply vehicle in 1QFY16.
- The Army began the M109 FoV PIM IOT&E in October 2016 at Fort Hood, Texas, but suspended testing after one of three test vignettes to determine the root cause of the toxic fumes coming into the cab of the howitzer. That effort continues. DOT&E will submit an IOT&E report in 2QFY17. A second IOT&E will be rescheduled for FY18 once corrective actions are complete.

Assessment

- Over the course of the Developmental Performance, Automotive, and LFT&E program, the Program Office has taken considerable action to correct deficiencies identified in early testing and to validate associated fixes.
  - During armor exploitation testing, most of the modified armored areas demonstrated that they provide protection against Key Performance Parameter threats.
  - Changes to the crew compartment Automatic Fire Extinguisher System (AFES) in the CAT mitigate the deficiency identified in early testing and reduce the CAT's vulnerability to fires.
- The crew compartment AFES in the SPH was designed to protect a small, localized area in the crew compartment. Live fire testing demonstrated that the system is deficient in providing adequate fire survivability. The Program Office is developing courses of action to redesign this system and improve SPH survivability to fires. While not yet optimized, the M109A7 provides improved crew fire safety compared to the currently fielded M109A6 because:
  - The M109A7 has crew compartment AFES capability while the M109A6 has none.
  - The M109A7 has reduced fire hazards compared to the M109A6 because of the replacement of hydraulic systems, found on the M109A6, with electric drives.
- The Army verified that the base SPH has the potential to provide underbody IED protection against the requirement blast threat and the objective level threat when equipped with the underbody blast kit.
- Reliability issues found on both the CAT and the SPH have been addressed in a comprehensive test-fix-test cycle throughout the PQT phase.
- Legacy system (parts common to the current M109A6) failures involving breech componentry and primer failures continue to arise in live fire testing and will not be addressed until follow-on developmental work is completed. Engine component failures in both the CAT and the SPH have been initially traced to transmission oil cooler design discrepancies. An interim design change has mitigated further failures and additional testing is ongoing. A final design change will occur during full-rate production.

Recommendations

- Status of Previous Recommendations. In FY15, the Army made design changes to mitigate the deficiencies in the CAT's crew compartment AFES and validated those changes in test. The Army has not yet incorporated changes to address the deficiencies in the SPH's crew compartment AFES but has developed and is reviewing several courses of action to address this issue.
- FY16 Recommendations. The Army should:
  1. Continue development of breech component upgrades and verify corrections for both the breech and engine deficiencies in testing.
  2. Correct the deficiencies in the SPH's crew compartment AFES and validate those fixes in test.

Mid-Tier Networking Vehicular Radio (MNVR)

Executive Summary

- In April through May 2016, the Army's Brigade Modernization Command (BMC) conducted a Mid-Tier Network and Mid-Tier Networking Vehicular Radio (MNVR) Operational Assessment (OA) as part of the Network Integration Evaluation (NIE) 16.2. The BMC assessed the concept of operations and basis of issue of a brigade's MNVR network operating in and out of a satellite-denied environment. The Army's assessment was not conducted according to a DOT&E-approved test plan, but DOT&E did observe the entire assessment and wrote an independent MNVR evaluation.
- The Army's BMC assessment of the NIE 16.2 MNVR OA is the following:
  - Recommend continued development of the mid-tier network solution to bridge the upper and lower tactical internets. Commanders validated the Army requirement for a mid-tier network solution.
  - Recommend the Army not field the MNVR as the mid-tier network solution. The limitations of the MNVR did not meet commanders' requirements to include the ability to provide consistent and reliable mission command services, maintain an effective operational range, and integrate into appropriate combat platforms.
- DOT&E's evaluation of the NIE 16.2 MNVR OA is the following:
  - MNVR did not meet commanders' requirements for a mid-tier network solution. Statistical analysis of NIE 16.2 results demonstrated there was no significant difference in the ability of commanders to accomplish their missions having the MNVR and not having the radio in a satellite-denied environment.
  - Commanders desired a 16-kilometer range for the mid-tier network, which is substantially further than the 6 – 10 kilometer requirement in the MNVR Capabilities Production Document. During NIE 16.2, infantry companies and cavalry troops operated in excess of 10 kilometers forward of their battalions for over 60 percent of the exercise.
  - The Army needs to conduct a complete IOT&E to test all features of MNVR and Joint Enterprise Network Manager (JENM) within an operationally representative unit.
- In July 2016, DOT&E approved the MNVR Test and Evaluation Master Plan (TEMP) in support of a September 2016 Milestone C decision to describe post-Milestone C developmental testing and an MNVR IOT&E.
- In September 2016, the Defense Acquisition Executive approved a low-rate initial production (LRIP) of 478 MNVRs. The Army intends to field the LRIP MNVRs to five Infantry Brigade Combat Teams (IBCTs), which far exceeds the one-brigade set needed to support the MNVR IOT&E.

- In September 2016, the Army published a new MNVR competitive acquisition that shifts the MNVR IOT&E to FY20. The new MNVR competitive acquisition is scheduled for a source selection against revised MNVR requirements and contract award in FY18-19. The results of this acquisition effort will likely result in a different radio and waveform to meet the Army's modified requirements and therefore, be of significantly different design than the LRIP MNVRs fielded to the five IBCTs.
- The Army needs to revise the approved MNVR TEMP to reflect the Army's new competitive strategy and testing that leads to an FY20 MNVR IOT&E.

System

- The Army's AN/VRC-118 MNVR program evolved from the terminated Joint Tactical Radio System, Ground Mobile Radio to provide software-programmable digital radios to support Army tactical communications requirements from company through brigade.
- The Army intends the MNVR to:
  - Operate at various transmission frequencies using the Soldier Radio Waveform (SRW) and the Wideband Networking Waveform (WNW).
  - Bridge the upper tactical communications networks at brigade and battalion with the lower tactical networks at company employing a terrestrial radio network.
  - Provide an alternative terrestrial transmission path in the absence or limited availability of satellite communications.
- The MNVR operates up to 75 watts maximum power output for WNW and up to 50 watts maximum power output for SRW.
- The JENM provides the means to plan, load, configure, and monitor MNVR networks.
- The MNVR includes both vehicle-mounted and Tactical Operations Center kit versions.

- The MNVR is a non-developmental item selected through multi-vendor competition.

Mission

- Army commanders intend to use the MNVR to:
  - Provide networked communications for host vehicles and Tactical Operations Centers during all aspects of military operations
  - Communicate and create terrestrial radio networks to exchange voice, video, and data using the SRW and the WNW.
  - Share data between different tactical communication networks and mission command systems
- Signal staffs employ the JENM to plan, load, monitor, control, and report on network operations of MNVR networks running SRW and WNW.

Major Contractor

Harris Corporation, Tactical Communications – Rochester, New York

---

Activity

- In November 2015, the Army conducted the MNVR Government Regression Test (GRT) at the Electronic Proving Ground in Fort Huachuca, Arizona. The GRT tested fixes to deficiencies discovered during the April to May 2015 NIE 15.2 MNVR Limited User Test and previous developmental testing, and assessed new MNVR capabilities. During the GRT, MNVR:
  - Demonstrated WNW and SRW data requirements
  - Demonstrated JENM configuration and over-the-air management of the MNVR
  - Was interoperable with Advanced Field Artillery Tactical Data System, Nett Warrior, and Joint Battle Command – Platform (JBC-P)
  - Met reliability requirements for all waveforms except the WNW anti-jam waveform
  - Did not demonstrate significant improvement in cybersecurity
- In April through May 2016, the Army BMC conducted a Mid-Tier Network and MNVR OA during NIE 16.2. During the MNVR OA, the Army equipped the 2nd Brigade, 1st Armored Division with MNVRs. The brigade headquarters and six battalions conducted missions under operationally realistic conditions. The BMC assessed the concept of operations and basis of issue of the MNVR network operating in and out of a satellite-denied environment. The mid-tier network and MNVR operated as part of the larger NIE 16.2 network during the OA, which included Warfighter Information Network – Tactical (WIN-T) Net Centric Waveform (NCW) satellite and JBC-P Blue Force Tracker (BFT) satellite. The Army's BMC assessment was not conducted according to a DOT&E-approved test plan, but DOT&E did observe the entire assessment and wrote an independent MNVR evaluation.
- In July 2016, DOT&E approved the MNVR TEMP in support of a September 2016 Milestone C decision to describe post-Milestone C developmental testing and an MNVR IOT&E.
- On July 5, 2016, DOT&E published a report on the results of BMC's NIE 16.2 Mid-Tier Network and MNVR OA.
- In September 2016, the Defense Acquisition Executive approved an LRIP of 478 MNVRs. The Army intends to field the LRIP MNVRs to five IBCTs, which far exceeds the one-brigade set needed to support the MNVR IOT&E.
- In September 2016, the Army published a new MNVR competitive acquisition that shifts the MNVR IOT&E to FY20. The new MNVR competitive acquisition is scheduled for a source selection against revised MNVR requirements and contract award in FY18-19.

Assessment

- The Army's BMC assessment of the NIE 16.2 MNVR OA is the following:
  - Recommend continued development of the mid-tier network solution to bridge the upper and lower tactical internets. Commanders validated the Army requirement for a mid-tier network solution.
  - Recommend the Army not field the MNVR as the mid-tier network solution. The limitations of the MNVR did not meet commanders' requirements to include the ability to provide consistent and reliable mission command services, maintain an effective operational range, and integrate into appropriate combat platforms.
- DOT&E's evaluation of the NIE 16.2 MNVR OA is the following:
  - MNVR did not meet commander's requirements for a mid-tier network solution.
  - Statistical analysis of NIE 16.2 results demonstrated there was no significant difference in the ability of commanders to accomplish their missions having the MNVR and not having the radio in a satellite-denied environment.
  - Commanders did not detect a difference between having the MNVR and not having the MNVR when the BFT and NCW satellite were off.
  - Having the brigades full authorization of MNVRs (85 nodes) did not improve mid-tier communications.
  - Commanders desired a 16-kilometer range for the mid-tier network.
  - The MNVR Capabilities Production Document requirement is 6 – 10 kilometers.
  - During NIE 16.2, infantry companies and cavalry troops operated in excess of 10 kilometers forward of their battalions for over 60 percent of the exercise.

- Commanders identified a need for a mid-tier network, but not the one provided by the MNVR WNW network.
- Soldiers identified position location information and text messaging as the most important messages. These messages do not require the bandwidth provided by WNW.
- MNVR requires more power to operate than legacy radio equipment. This requires vehicles to maintain continuous idle during MNVR operations.
- MNVR is too large and draws too much power to be integrated into the leader vehicles (Abrams and Bradley).

• The results of the new MNVR competitive acquisition effort will likely result in a different radio and waveform to meet the Army's modified requirements and therefore, be of significantly different design than the LRIP MNVRs fielded to the five IBCTs.

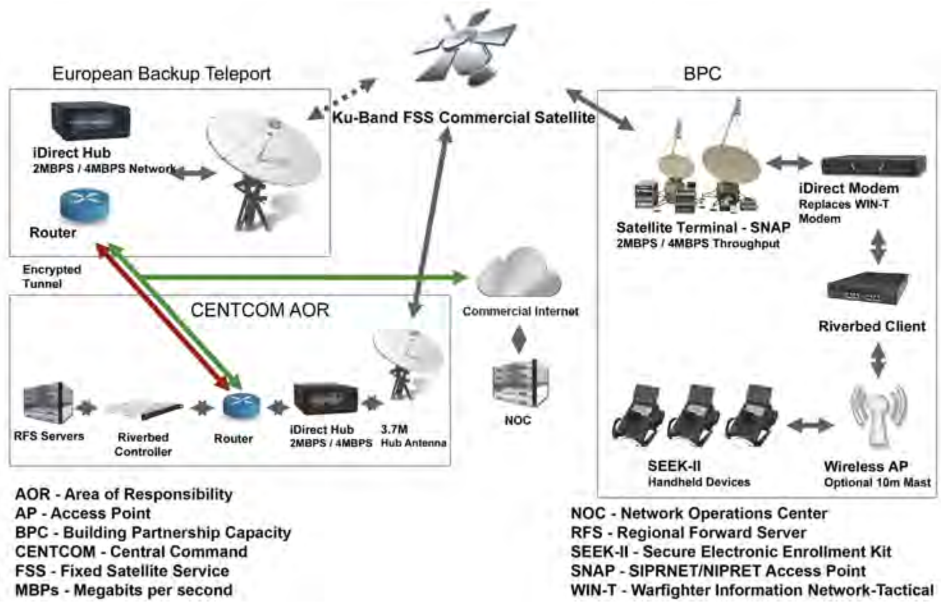
• Due to the program changes resulting from the MNVR competitive acquisition, the Army needs to revise the approved MNVR TEMP to reflect the Army's MNVR competitive source selection and testing leading to a FY20 MNVR IOT&E.

Recommendations

• Status of Previous Recommendations. The MNVR Program Office has addressed the previous recommendations to continue development and develop a Milestone C TEMP. Planning of the IOT&E has continued.

• FY16 Recommendations. The Army should:
  1. Reevaluate MNVR transmission range and throughput requirements to reflect operational mission needs of the unit.
  2. Revise its post-Milestone C MNVR TEMP to reflect the developmental test and activities leading to the planned FY20 MNVR IOT&E.
  3. Plan and conduct an MNVR IOT&E using an IBCT equipped with WIN-T, JBC-P, and MNVR in accordance with an Army-approved MNVR basis of issue plan.

Near Real Time Identity Operations (NRTIO)



Executive Summary

- Near Real Time Identity Operations (NRTIO) is a Joint Emerging Operational Need (JEON) intended to provide the following capabilities to U.S. Central Command (USCENTCOM) in support of Operation Inherent Resolve:
  - Near real-time identity information to U.S. conventional forces to enhance force protection, stem the flow of foreign fighters, and counter the threat from IEDs
  - Increased partnership capacity by sharing collected biometric data with partner nations and other coalition forces to establish the identity of adversaries transiting the USCENTCOM Area of Responsibility (AOR)
- NRTIO achieved Initial Operating Capability (IOC) in February 2016, and the Army Test and Evaluation Command (ATEC) conducted an IOC operational assessment (OA) from March through July 2016 using data from the USCENTCOM AOR.
- Test limitations precluded the assessment of operational effectiveness, operational suitability, and cybersecurity during the IOC OA, including:
  - Due to the IOC state of NRTIO, soldiers could not use its full capability. The biometric dataset on the Remote Forward Server (RFS) was incomplete, which reduced the rate of biometric submission matches against the biometrically enabled watchlist (BEWL). The IOC OA demonstrated that biometric submissions to the RFS had a lower than acceptable match accuracy.
  - To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size.
  - USCENTCOM did not permit cybersecurity testing on the production hardware and software due to mission constraints.
- During the IOC OA, soldiers successfully completed enrollments and matches with their local collection device against watchlists on the NRTIO RFS and the DOD authoritative database (Automated Biometric Identification System (ABIS)). Due to IOC OA constraints, RFS response timeliness could not be adequately assessed. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated but the sample size is not statistically significant.
- Prior to reaching Full Operating Capability (FOC), NRTIO requires a technical modernization to improve the accuracy and completeness of the RFS biometric dataset. An accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR is necessary to demonstrate near real-time identity operations.

System

The NRTIO JEON intends to provide the forward-deployed Service member the capability to receive an identity response in near real-time of submission of biometric information. The IOC OA configuration includes:

- Handheld Biometric Collection devices. The Secure Electronic Enrollment Kit (SEEK) II performs fingerprint capture, dual iris scan, and facial capture. The devices are compliant with Electronic Biometric Transmission Specification (EBTS) and Electronic Fingerprint Transmission Specification (EFTS), which are requirements for interface with ABIS.
- Dedicated communications capacity including tactical satellite (TACSAT), satellite communications (SATCOM), and WiFi connectivity.
- RFS. The RFS includes the USCENTCOM AOR-specific biometric records that allow for rapid, non-authoritative match results to be provided to the forward deployed warfighter. ABIS verifies the biometric matches using the authoritative database, which possesses a larger dataset.
- Web-based Exploitation and Analysis Portal. An identity operations portal that provides web-based real-time collaboration, automated report generation, materiel management, data search and correlation, alerting, and a database for exploitation and collaboration. The portal used

during the IOC OA was the Identity Resolution Exploitation and Management Services Collaborative Workstation (ICW).

Mission

- USCENTCOM forces use the NRTIO IOC capability for identity operations to provide timely, accurate, and complete responses indicating whether persons of interest encountered in the field have a prior history of derogatory (e.g. criminal) activity, to assist in identifying potential threats to U.S. forces and facilities throughout the USCENTCOM AOR.
- Upon achieving FOC, forward-deployed Service members will use NRTIO to provide biometric responses including tailored biometric matching and watchlisting within the USCENTCOM AOR.

Major Contractors

- Booz Allen Hamilton – Belcamp, Maryland
- Envistacomm LLC – Atlanta, Georgia

Activity

ATEC conducted the following testing in FY16:

- The IOC OA of the NRTIO system from March to July 2016
- A cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) during developmental testing of a clone of the IOC portal, one component of the NRTIO, in July 2016

Assessment

- The IOC OA leveraged the operational assessment process of the JEON and focused on whether the technology is viable to meet the warfighter requirements and will be used to inform the tailored Test and Evaluation Master Plan (TEMP) and operational test plan to support FOC. At the FOC OA, the operational assessment will focus on the operational effectiveness, suitability, and survivability of the NRTIO system under test. Accordingly, the test needs to have a DOT&E-approved test plan and tailored TEMP.
- During the IOC OA, the biometric dataset on the RFS was incomplete, which reduced the rate of biometric submission matches against the BEWL. To meet mission timelines, ATEC started operations on the RFS without the complete biometric and latent dataset relevant to the USCENTCOM AOR. Match consistency between the RFS and ABIS is a key criterion for establishing operator confidence in the RFS. If biometric matches are missed by the RFS, a potential person of interest may not be identified. The RFS technology limitation of having not fully ingested the entire biometric database precluded assessment of the dynamic synchronization of the DOD BEWL with the RFS.
- Due to IOC OA constraints, DOT&E could not adequately assess RFS response timeliness. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated. However, the majority of the IOC OA biometric enrollments were submitted using a bulk file upload to the portal, which forwarded the data on to both ABIS and the RFS. Bulk uploading of biometric submissions is adequate for many operational needs.
- To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size. Survey responses noted suitability problems that included high workloads including periods of enrollment surges, long upload times, and communications outages. There were many non-materiel shortcomings. Areas to address to improve suitability include lack of leadership awareness of the importance of biometrics, the need for intensive training of soldiers with no prior biometrics experience, and transportability hardships because of the hostile terrain in parts of the USCENTCOM AOR.
- ABIS operators at the Biometrics Identity Management Agency reviewed over 800 NRTIO biometric enrollments to assess whether soldiers were able to collect biometric data of match quality. For the NRTIO biometric enrollments, fingerprint quality was generally acceptable for obtaining accurate matches, whereas iris and facial images showed greater variability. Since most matches primarily rely on fingerprint data, the data quality of NRTIO biometric enrollments was adequate to support identity operations.
- Mission constraints prevented an adequate assessment of the cybersecurity posture during the ATEC-conducted CVPA on a clone of the ICW.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
    1. Mature tactics, techniques, and procedures and address manpower requirements to improve suitability prior to FOC.
    2. Prior to FOC operational testing, load the current USCENTCOM subset of the BEWL on their SEEK IIs, so watchlisted individuals can be identified in near real-time.
    3. For FOC, streamline or automate training to improve the suitability of NRTIO.
    4. Conduct an operational CVPA and Adversarial Assessment on the NRTIO system including the RFS prior to FOC.
    5. Complete a technical modernization of the NRTIO system that has an accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR prior to FOC.
    6. Provide an operational test plan and tailored TEMP 30 days prior to the start of the FOC OA to DOT&E for approval.

Patriot Advanced Capability-3 (PAC-3)

Executive Summary
- The Army completed the Patriot Post-Deployment Build-8 (PDB-8) Developmental Test and Evaluation (DT&E) from July 2015 to July 2016.
- The Army conducted four Patriot flight tests and two Army Integrated Air and Missile Defense (AIAMD) flight tests using Patriot interceptors in FY16, achieving successful intercepts of all targets: five short-range ballistic missile (SRBM) targets, three cruise missile targets, and one fixed-wing aircraft target.
- The Army commenced the Patriot PDB-8 IOT&E in September 2016. This testing will continue through August 2017.

System
- Patriot is a mobile air and missile defense system that counters missile and aircraft threats. The newest version of Patriot hardware and software under development is PDB-8, which consists of improvements required to counter the evolving threat, to improve combat identification and the Air Defense Interrogator Mode 5 Identification, Friend or Foe (IFF) capability, to mitigate false tracks, to improve electronic protection, and to further integrate Missile Segment Enhancement (MSE) interceptor/ground system capabilities.
- The system includes the following:
  - C-band multi-function phased-array radars for detecting, tracking, classifying, identifying, and discriminating targets and supporting the guidance functions
  - Battalion and battery battle management elements
  - Communications Relay Groups and Antenna Mast Groups for communicating between battery and battalion assets
  - A mix of Patriot Advanced Capability-3 (PAC-3) hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors for negating missile and aircraft threats
- The newest version of the PAC-3 interceptor under development is the PAC-3 MSE. The MSE provides increased battlespace defense capabilities and improved lethality over prior configuration Patriot interceptors.
- Earlier versions of Patriot interceptors include the Patriot Standard interceptor, the PAC-2 Anti-Tactical Missile, the Guidance Enhanced Missile (GEM) family (includes the GEM-T and GEM-C interceptor variants intended to counter tactical ballistic missiles and cruise missiles), the PAC-3 (baseline), and the PAC-3 Cost Reduction Initiative (CRI) variant.

Mission
Combatant Commanders use the Patriot system to defend deployed forces and critical assets from missile and aircraft attack and to defeat enemy surveillance air assets in all weather conditions and in natural and induced environments.

Major Contractors
- Prime: Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts (ground system and PAC-2 and prior generation interceptors)
- PAC-3, PAC-3 CRI, and PAC-3 MSE Missiles: Lockheed Martin Corporation, Missile and Fire Control – Grand Prairie, Texas

Activity
- The Army conducted the Patriot PDB-8 DT&E from July 2015 to July 2016 at White Sands Missile Range (WSMR), New Mexico. The ground portion of this testing concluded in October 2015, with developmental flight tests occurring later:
  - In Flight Test P8-2 in November 2015, Patriot conducted a mixed ripple engagement of an SRBM target with PAC-3 CRI and PAC-2 GEM-T interceptors and then engaged a second SRBM target with two PAC-2 GEM-T interceptors.
  - In Flight Test P8-4 in December 2015, Patriot engaged an SRBM target with two PAC-3 MSE interceptors.
  - In Flight Test P8-3 in March 2016, Patriot conducted a mixed ripple engagement of an SRBM target with PAC-3 MSE and PAC-2 interceptors.
  - In Flight Test P8-1 in July 2016, Patriot engaged a cruise missile target with a PAC-2 GEM-T interceptor and then

engaged a maneuvering, full-scale, fixed-wing, air-breathing target with a PAC-3 MSE interceptor. The Army did not conduct this test in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP), which stated that the fixed-wing aircraft would be employing electronic countermeasures while maneuvering. The Army has deferred testing of this capability to a Patriot PDB-8.1 flight test in 2020.

- The Army conducted two AIAMD flight tests at WSMR during FY16 using Patriot interceptors:
  - In AIAMD Flight Test-1 (FT-1) in November 2015, Patriot engaged a cruise missile target with a PAC-3 interceptor.
  - In AIAMD FT-3 in April 2016, Patriot engaged an SRBM target with one PAC-3 interceptor and conducted two separate PAC-2 GEM-T engagements against a cruise missile target, with the first engagement resulting in a missed intercept and the second engagement resulting in a successful intercept.
- The Army conducted lethality testing of the PAC-3 MSE lethality enhancer titanium fragments against Composition B explosive from July 2015 through June 2016 at Aberdeen Proving Ground, Maryland, to update the lethality model that predicts when a high-explosive initiation occurs within a warhead impacted by fragments.
- The Army conducted all testing in accordance with the DOT&E-approved TEMP and/or test plans, with the exception of the previously discussed P8-1 flight test and the PDB-8 flight test against an anti-radiation missile, which the Army deferred to a Patriot PDB-8.1 flight test in 2021 due to the lack of an available target.
- The Army commenced the Patriot PDB-8 IOT&E in September 2016 at Yuma Proving Ground, Arizona. The IOT&E, which will include flight tests conducted at WSMR and the Reagan Test Site at the Kwajalein Atoll in the Marshall Islands, will continue through August 2017. The IOT&E will provide information to support the PAC-3 MSE Full-Rate Production decision and the Army's deployment of Patriot PDB-8.
- The 2016 National Defense Authorization Act directs that the Missile Defense Agency and the Army conduct at least one intercept flight test each year that demonstrates interoperability and integration among the covered air and missile defense capabilities of the United States. In response to this act, Aegis Ballistic Missile Defense (BMD) will participate in Patriot's final operational flight test in FY17 as a forward-based sensor.

Assessment

- Problems previously discovered during the PDB-7 Limited User Test (LUT), if not corrected by the Army, could adversely affect Patriot PDB-8 effectiveness, suitability, or survivability. These problems, the details of which can be found in DOT&E's classified April 2013 Patriot PDB-7 LUT report, include:
  - Patriot PDB-7 performance against some threats improved compared to PDB-6.5, but there were degradations in performance against other threats. Patriot had some effectiveness shortfalls.
  - Patriot ground system reliability did not meet the threshold requirement, but would have met it had the Patriot radar achieved its allocated reliability goal.
  - Patriot ground system maintainability did not meet the threshold requirement.
  - Patriot training remained inadequate to prepare operators for complex Patriot engagements. This was also true during the PDB 6.5 and PDB-6 LUTs.
  - Patriot had some survivability and cybersecurity shortfalls.
- The Patriot system met most of its test objectives during the Patriot PDB-8 DT&E, but not all. During the ground test portion using simulated interceptors and mostly simulated targets, Patriot did not always properly transmit messages; detect, classify, and discriminate targets; or select the preferred interceptors against targets (e.g., Patriot would sometimes incorrectly select a PAC-2 GEM against a fast tactical ballistic missile or a PAC-3 interceptor against a threat aircraft).
  - There were anomalies in the Patriot PDB-8 implementation of IFF, which led to over-interrogations and indicated degradation from the previously demonstrated PDB-7 IFF capability. The Army updated the PDB-8 software to correct these problems and the fixes will be verified during IOT&E.
  - Patriot PDB-8 Training Software sometimes generated spurious alerts and improperly displayed some scripted targets.
  - The Patriot system did not meet its reliability requirements during this test.
- During Flight Test P8-2, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with a mixed ripple method of fire using PAC-3 CRI and PAC-2 GEM-T interceptors and a second SRBM target with two PAC-2 GEM-T interceptors. In both instances, the first interceptor in the ripple intercepted and killed the target at the planned altitude, and performance of the ground system and interceptor was nominal.
- During Flight Test P8-4, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with two PAC-3 MSE interceptors. The first PAC-3 MSE intercepted and killed the target at the planned altitude, and performance of the ground system and interceptor was nominal, although some post-intercept ground system anomalies occurred that did not affect the mission objectives.
- During Flight Test P8-3, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with a mixed ripple method of fire using a PAC-3 MSE and a PAC-2 GEM-T interceptor. The PAC-3 MSE (the first interceptor) intercepted and killed the target at the planned altitude and both ground system and interceptor performance was generally nominal, although a Link-16 network initialization problem prevented the demonstration of Patriot PDB-8 interoperability on Link-16 during this flight test. Other parts of the Patriot PDB-8 DT&E demonstrated Link-16 interoperability.

- During Flight Test P8-1, Patriot demonstrated the capability to detect, track, engage, intercept, and kill a low-radar cross section cruise missile target at low altitude and in a clutter environment with a PAC-2 GEM-T interceptor and, following this, a maneuvering full-scale aircraft target with a PAC-3 MSE interceptor. The interceptors killed both targets at the planned ranges and altitudes, and performance of the ground system and interceptors were nominal for both engagements. Patriot demonstrated PDB-8 interoperability on Link-16 during this flight test.
- During AIAMD FT-1, Patriot demonstrated the capability to engage, intercept, and kill a low-altitude cruise missile target with a PAC-3 interceptor based on remote Sentinel radar data sent through an AIAMD Battle Command System Engagement Operations Center.
- During AIAMD FT-3, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target using a PAC-3 interceptor and a cruise missile target with the second of two PAC-2 GEM-T interceptors after the first GEM-T missed.
- The PAC-3 MSE lethality enhancer testing showed that the existing lethality model for titanium did not predict, within 10 percent of the observed critical velocities, when a high-explosive initiation of a warhead would occur. The Army used these results to develop new coefficients for their lethality model that more accurately represent the PAC-3 MSE titanium fragments.

Recommendations

- Status of Previous Recommendations. The Army satisfactorily addressed 15 of the previous 23 recommendations. The Army should continue to address the following recommendations:
  1. Conduct Patriot air and missile defense testing during joint and coalition exercises that include large numbers of different aircraft types, sensors, battle management elements, and weapons systems. Additionally, the Army should conduct Red Team Adversarial Assessments during joint exercises to test Patriot cybersecurity.
  2. Conduct a Patriot flight test against an anti-radiation missile target to validate models and simulations.
  3. Improve Patriot training to ensure that Patriot operators are prepared to use the system in combat.
  4. Have Patriot participate with live interceptors in Terminal High Altitude Area Defense (THAAD) flight testing to determine Patriot-to-THAAD interoperability and the capability for Patriot to intercept tactical ballistic missile targets that THAAD does not intercept.
  5. Collect operational reliability data on Patriot systems in the field so that the Mean Time Between Critical Mission Failure can be calculated.
  6. Use test units for future Patriot operational tests that have operationally representative distributions in soldier proficiency.
  7. Conduct future operational flight tests with unannounced target launches within extended launch windows.
  8. Improve Patriot radar reliability.
- FY16 Recommendations. The Army should:
  1. Conduct a simultaneous engagement of a cruise missile target with a PAC-2 GEM-T interceptor and a maneuvering full-scale fixed-wing aircraft target employing electronic countermeasures with a PAC-3 MSE interceptor.
  2. Have Patriot participate with live interceptors in Aegis BMD flight testing to determine Patriot-to-Aegis BMD interoperability and the capability for Patriot to intercept ballistic missile targets that Aegis BMD does not intercept.

Soldier Protection System (SPS)

Executive Summary

- The Soldier Protection System (SPS) is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights.
- The SPS consists of four subsystems: soft armor Torso and Extremity Protection (TEP); hard armor Vital Torso Protection (VTP); the Integrated Head Protection System (IHPS); and Transition Combat Eye Protection (TCEP). Each SPS subsystem is compatible with existing personal protective equipment. The Army plans to add SPS to Deployer Equipment Bundles for issue to deploying units rather than issue SPS to individual soldiers at an Army installation.
- The Army made a Full-Rate Production decision for the TEP and a Milestone C decision for IHPS and TCEP in September 2016. The Army plans to make separate Full-Rate Production decisions for the VTP in July 2017 and IHPS in April 2018. The Army plans to make the TCEP available for unit purchase rather than to field it across the Army.
- The Army completed testing the TEP and began testing the VTP subsystem in 2016. The Army completed developmental testing of the IHPS in 2016, and awarded a low-rate initial production contract for IHPS in 2016. The Army will continue testing both the VTP and IHPS in FY17.
- Compared to the current Improved Outer Tactical Vest, the SPS TEP provides similar protection at a reduced weight against the threats tested.

System

- The SPS is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights. The SPS subsystems are designed to protect a soldier's head, eyes, and neck region; the vital torso and upper torso areas, as well as the extremities; and the pelvic region. Soldiers can configure the various components to provide different tiers of protection depending on the threat and the mission.
- The SPS consists of four subsystems:
  - VTP consists of front and rear hard armor torso plates (either the Enhanced Small Arms Protective Insert (ESAPI) or the X Threat Small Arms Protective Insert (XSAPI)), along with the corresponding hard armor side plates (Enhanced Side Ballistic Insert (ESBI) or the X Threat Side Ballistic Insert (XSBI))
  - TEP consists of the soft armor Modular Scalable Vest (MSV) with provision for adding the Ballistic Combat Shirt (BCS) for extremity protection, the Blast Pelvic Protector (BPP) for pelvic and femoral artery protection, and a Load Distribution System (LDS) for the capability to redistribute the weight burden from the shoulders to the hips
  - IHPS consists of a helmet, with provision for adding a mandible and/or visor, as well as for mounting an applique to the outside of the helmet for additional ballistic protection
  - TCEP consists of either ballistic spectacles or goggles to protect the soldier's eyes as well as provide the capability to transition from light to dark and dark to light in one second or less to enhance the soldier's vision in varying combat conditions

- The Army initially plans to add SPS to Deployer Equipment Bundles for issue to deploying units rather than issue SPS to individual soldiers at each Army installation.

Mission

Units with soldiers wearing the SPS will accomplish assigned missions while concurrently protecting themselves against injury from a variety of ballistic (small-arms and fragmenting) threats.

Major Contractors

- TEP LRIP Vendors/Designs (Multiple vendors to stimulate competition and achieve best price through Fair Opportunity awards):
  - KDH Defense Systems INC – Eden, North Carolina (MSV, BPP)
  - Bethel Industries Inc. – Jersey City, New Jersey (MSV, BPP)
  - Hawk Protection – Pembroke Pines, Florida (MSV, BPP)
  - Short Bark Industries – Venor, Tennessee (BCS)
  - Carter Enterprises Industries Inc. –Brooklyn, New York (LDS, BCS)
  - Eagle Industries Unlimited – Virginia Beach, Virginia (BCS)
- IHPS Vendors (developmental testing awardees):
  - 3M/Ceradyne – Costa Mesa, California
  - Gentex – Simpson, Pennsylvania
  - Revision Military –Essex Junction, Vermont
- VTP LRIP Vendors:
  - BAE Systems – Chandler, Arizona (XSAPI, ESBI, XSBI)
  - 3M/Ceradyne – Costa Mesa, California (ESAPI)

Activity

- While the SPS consists of four subsystems (TEP, VTP, IHPS, and TCEP), the development, testing, and production/fielding of the four subsystems are on different timelines. The Army made a Full-Rate Production decision for TEP and a Milestone C decision for IHPS and TCEP in September 2016, and plans to make separate Full-Rate Production decisions for the VTP in July 2017 and IHPS in April 2018. The Army plans to make TCEP available for unit purchase rather than to field it across the Army. Each SPS subsystem is compatible with existing (legacy) personal protective equipment (for example, soldiers can use existing hard armor plates in the new MSV). The Army is testing SPS ballistic performance in accordance with DOT&E-approved LFT&E test plans.
- The Army completed TEP testing in July 2016, to support the TEP Full-Rate Production decision. TEP testing included:
  - IOT&E of the TEP in March 2016, at Fort Hood, Texas, to assess the impact of the TEP on soldier mobility and subsequent mission effectiveness.
  - A series of first article and sub-system level live fire testing of the TEP from January through July 2016. Sub-system level testing included testing of the MSV with currently fielded hard armor plates, and testing of the MSV/hard armor subsystem against foreign threats. Testing also included a series of blast testing events to characterize the performance of the TEP and current hard armor plates when subjected to blast events. The Army also conducted flash heat and fire threat testing to evaluate the TEP's ability to protect an individual from burns resulting from a flash fire.
  - The Army used data from first article testing to model the ability of the TEP to protect the wearer from serious injury from fragments perforating the TEP.
- The Army began VTP testing in December 2015, with first article testing of the ESAPI hard armor plates. Shortly thereafter, the Army halted further ESAPI testing because test personnel found deficiencies in the plates while conducting physical characterization of the plates prior to starting ballistic testing. Following a period of corrective action, the vendor resubmitted the ESAPI plates for first article testing, which occurred from July through August 2016. The Army conducted first article testing of the ESBI, XSBI, and XSAPI hard armor plates in May 2016. The XSAPI plate did not meet the ballistic requirements. The Army is waiting for the vendor to complete corrective actions and resubmit the XSAPI for another first article test. XSAPI resubmission is unknown at this time. The Army will continue VTP testing in FY17.
- The Army completed a third round of IHPS developmental testing in April 2016. The Army awarded a low-rate initial production contract for IHPS in September 2016. The Army will continue IHPS testing in FY17.
- The Army conducted technical and user testing of TCEP in FY16. The Army will continue TCEP testing in FY17.

Assessment

- IOT&E results indicate that some soldiers had trouble aiming their weapons when wearing the BCS and LDS with the MSV while in a prone firing position. Additionally, some female soldiers experienced restricted upper-body movement due to ill-fitting and uncomfortable BCS.
- The SPS TEP met its ballistic requirements against the threats tested.
- Compared to the currently fielded Improved Outer Tactical Vest, the SPS TEP provides similar protection at a reduced weight against the threats tested.
- Wearing body armor reduced the peak overpressure behind the armor during blast testing, but additional investigation is needed to understand how the pressure data can be analyzed and correlated to injury.
- TEP modeling required extrapolation of test data to estimate performance, which added uncertainty in evaluation of TEP performance for those conditions. The use of a broader range of fragment masses to more fully represent a threat would: provide additional test data to support future modeling efforts; make such extrapolation unnecessary; and improve confidence

in the modeling results and subsequent conclusions made about TEP performance.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Improve the design of the LDS so it does not interfere with the wearer's ability to properly aim a weapon. The Army should also provide BCS sizes and designs that correctly fit all female soldiers and are comfortable to wear.
  2. Continue to improve its body armor blast testing and analysis procedure. Improvements should include determining whether results can be correlated to injury.
  3. Use a broader range of fragment simulators to more fully represent the expected threat environment and to then more fully characterize TEP performance.
  4. Quantify the uncertainty associated with its modeling estimates and assess the impact of that uncertainty on the evaluation of TEP performance. This should include additional end-to-end testing of an actual threat (not just representative fragments) against the actual TEP as represented in the model.

Spider Increment 1A M7E1 Network Command Munition

Executive Summary

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy.
- Spider Increment 1A is an upgrade to the fielded Increment 1 system. The Increment 1A system has the requirement to fire anti-vehicular, obstacle-producing munitions and to operate seamlessly with mission command systems. The upgrade is backwards compatible with the Spider Increment 1 system and includes:
  - A new Remote Control Unit (RCU) with an enhanced colored map background
  - Updated software to promote ease of user operability
  - A Secure Mission Data Loader (SMDL)
  - An Interactive Electronic Training Manual (IETM)
- The Army conducted a Limited User Test (LUT) in 3QFY16. During the LUT, Spider Increment 1A demonstrated no new capability over the fielded system. Units accomplished their missions using Spider Increment 1A, but Increment 1A did not meet its reliability requirement and had cybersecurity vulnerabilities during the test.
  - Increment 1A demonstrated significant reliability problems during the LUT. The reliability threshold is 0.96 probability of having no failures during a 72-hour mission. During the LUT, the system computer achieved a 0.65 probability of completing a mission without a failure.
  - Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
  - Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network. The Army is in the process of changing the seamless interoperability requirement from a threshold to an objective requirement. The Army has not yet approved the change.

System

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directs the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- The Army fielded Spider Increment 1 systems in FY09 under an Urgent Materiel Release. The system reached Initial Operational Capability in FY11 and obtained its Full Materiel Release in FY13.
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities)
  - A remote control station, used by the operator to maintain "man-in-the-loop" control of all munitions in a field (this is the component upgraded in Increment 1A)
  - A communications relay device known as a Repeater for use in difficult terrain or at extended ranges
- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non combatants and has the capability to use non-lethal munitions such as the Modular Crowd Control Munition that fires rubber sting balls.

Mission

Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter-mobility obstacles using lethal and non-lethal munitions. Spider functions as a stand-alone system or when combined with other obstacles to accomplish the following:

- Provide early warning
- Protect the force
- Delay and attrit enemy forces
- Shape the battlefield

Major Contractor

Command and Control hardware and software: Northrop Grumman Information Systems Sector, Defense Systems Division – Redondo Beach, California

Activity

- In January 2016, the Army conducted a Cooperative Vulnerability and Penetration Assessment. This assessment identified four cybersecurity vulnerabilities.
- In March 2016, the Army conducted a System Verification Test at Fort Leonard Wood, Missouri. Multiple Software Change Requests were submitted to the contractor based on this test.
- During May 2016, the Army conducted the Spider Increment 1A LUT at the Network Integration Evaluation 16.2 at Fort Bliss, Texas, in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- During FY16, the Army continued its contract with Northrop Grumman to refine Spider Increment 1A software.
- At the end of FY16, the Army was updating the Spider Increment 1A TEMP to support a Milestone C decision and a projected IOT&E for FY18.

Assessment

- During the LUT, Spider Increment 1A demonstrated suitability and survivability deficiencies.
  - Operational effectiveness – A trained unit can employ Spider Increment 1A as a component of a protective obstacle and provide obstacle effects as intended by the commander.
  - Suitability – The system's computer did not demonstrate its reliability requirement during the LUT. The system is required to have a 0.96 probability of completing a 72-hour mission without failures. During the LUT, 13 of 20 missions had no essential function failures, resulting in the computer demonstrating a mission success rate of 0.65.
  - Survivability – Due to cybersecurity deficiencies, Spider Increment 1A components are not survivable in an operational environment.
- Based on the Capability Development Document, Spider Increment 1A demonstrated no new capability during the FY16 LUT.
  - Spider Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network.
  - A cross-domain solution that could enable two-way communication between unclassified and classified systems does not currently exist. The Army was aware of this cross-domain problem prior to the LUT and did not attempt to include this functionality during the test.
  - The Army is in the process of changing the Spider Increment 1A seamless interoperability requirement. The Program Office and user representatives propose downgrading the requirement from a threshold to an objective requirement. The Army has not yet approved the change.
- Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
- The Army did not correct all identified cybersecurity vulnerabilities prior to the LUT. The Army plans on addressing and testing all cybersecurity deficiencies prior to the IOT&E.

Recommendations

- Status of Previous Recommendations. The Army corrected Spider Increment 1 deficiencies addressed in previous recommendations.
- FY16 Recommendations. The Army should:
  1. Design the Spider Increment 1A IOT&E to enable the characterization of the system's end-to-end mission effectiveness, over the maximum operational distance, to inform the system operators of its capabilities and limitations in the various conditions that will be encountered during combat operations. These conditions should include cyber and electronic warfare.
  2. Include doctrine, tactics, and techniques on engagement area development in unit pre-IOT&E training. The maneuver unit commander should assume the responsibility to ensure leaders, soldiers, and the Spider equipped engineer unit are trained properly. Training should include a situational training exercise on collective tasks related to engagement area development augmented by an engineer unit resourced with Spider Increment 1A systems.
  3. Resolve the problem between Spider Increment 1A and the mission command system preventing Spider Increment 1A from sending digital obstacle reports to the classified mission command systems. This will allow units to know in real time where Spider fields are located on the battlefield.
  4. Prior to IOT&E:
     - Develop, fund, and implement a comprehensive reliability growth plan to correct system reliability deficiencies.
     - Demonstrate fixes to the RCU, RCU Transceiver, MCU, and Repeater reliability and communication issues through testing.
     - Develop fixes for the known cybersecurity vulnerabilities.

Warfighter Information Network – Tactical (WIN-T)

Executive Summary

- The Army Acquisition Executive (AAE) conducted a Warfighter Information Network – Tactical (WIN-T) Increment 3 decision review based upon the Network Integration Evaluation (NIE) 16.2 WIN-T Increment 3 Operational Assessment in September 2016. The DOT&E evaluation was:
  - Net Centric Waveform (NCW) satellite enhancements are operationally effective and provide improved support of mission command applications, increased bandwidth, and a stable network.
  - Network Operations (NetOps) enhancements were not operationally effective and, due to database failures, did not provide timely and accurate information to NetOps soldiers to conduct their WIN-T network mission. Some NetOps features – such as the NCW and Highband Networking Waveform (HNW) planning tools – enhanced the soldiers' ability to perform NetOps.
  - Due to complexity, the WIN-T Increment 3 tunnel-less architecture is not effective and adversely affected NetOps soldiers' planning, controlling, monitoring, and visualization functions.
  - The execution of NIE 16.2 WIN-T Increment 3 Operational Assessment was not adequate to assess operational suitability.
  - Although survivability has improved, WIN-T Increment 3 still has significant cybersecurity vulnerabilities.
- The WIN-T program took prompt action to resolve NetOps problems identified during operational test and demonstrated these fixes during a July 2016 contractor development test (CDT) conducted under benign conditions.
- In September 2016, the AAE approved the deployment of WIN-T Increment 3 NetOps and NCW enhancements.
- The Army is updating the WIN-T Increment 2 post-full-rate production Test and Evaluation Master Plan (TEMP) to include an FY17 FOT&E to test WIN-T Increment 2 configuration items designed to support light brigades with downsized, air-transportable WIN-T assemblages.

System

- The Army designed WIN-T as a three-tiered communications architecture (space, terrestrial, and airborne) to serve as the Army's high-speed and high-capacity tactical communications network.
- The Army intends WIN-T to provide reliable, secure, and seamless communications for units operating at theater level and below.
- The WIN-T program consists of three funded increments. In May 2014, the Defense Acquisition Executive approved the Army's request to stop development of the Increment 3 aerial tier of networked, airborne, communications relays and limit Increment 3 to network management and satellite waveform improvements. The Army intends to increase procurement of WIN-T Increment 2 configuration items to satisfy the number of capability sets previously planned for Increment 3.
  - Increment 1: "Networking At-the-Halt" enables the exchange of voice, video, data, and imagery throughout the tactical battlefield using a Ku- and Ka-satellite-based network. The Army has fielded WIN-T Increment 1 to its operational forces.
  - Increment 2: "Initial Networking On-the-Move" provides command and control on-the-move down to the company level for maneuver brigades and implements an improved network security architecture.
  - WIN-T Increment 2 supports on-the-move communications for commanders with the addition of the Point of Presence and the Soldier Network Extension, and provides a mobile network infrastructure with the Tactical Communications Node.
  - WIN-T Increment 2 provides a downsized, air transportable variant of High Mobility Multi-purpose Wheeled Vehicle (HMMWV) mounted configuration items to support the Army's Global Response Force and other light brigades.
  - Increment 3: "Full Networking On-the-Move" was to provide full mobility mission command for all Army field commanders, from theater to company level using networked airborne communication relays. With program reductions, WIN-T Increment 3 now provides enhanced NetOps and an improved satellite waveform to WIN-T Increments 1 and 2.

Mission

Commanders at theater level and below will use WIN-T to:

- Integrate satellite-based communications capabilities into an everything-over-Internet Protocol network to provide connectivity, while stationary, across an extended, non-linear battlefield, and at remote locations (Increment 1)
- Provide division and below maneuver commanders with mobile communications capabilities to support initial command and control on-the-move (Increment 2)

Major Contractor

General Dynamics, C4 Systems – Taunton, Massachusetts

Activity

- In October 2015, the Army conducted a WIN-T Increment 3 Government Developmental Test (GDT) of the enhanced Net-Centric Waveform 10.1.2b (NCW 10.x) at Aberdeen Proving Ground, Maryland. The GDT demonstrated that NCW 10.x could support 12 megabits per second (Mbps) throughput at the larger-dish Satellite Transportable Terminals, which support the WIN-T Increment 2 Tactical Communications Node.
- The Army conducted the final of three WIN-T Increment 3 functional qualification tests at the contractor's facility in December 2015. In the January 2016 report, the Army did not report any significant problems.
- In January and February 2016, the Army Test and Evaluation Center (ATEC) conducted an instrumentation accreditation event on the proposed instrumented data collection, reduction, and assessment (DCRA) process intended for use during the WIN-T Increment 3 Operational Assessment. The instrumentation accreditation event did not accredit the DCRA process, and ATEC continued efforts to fix DCRA problems into the NIE 16.2 WIN-T Increment 3 Operational Assessment.
- The Army conducted a WIN-T Increment 3 Operational Assessment during the May 2016 NIE16.2. The operational test employed the 2nd Brigade, 1st Armored Division conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. The operational assessment focused on WIN-T Increment 3 enhancements, including NetOps software tools and an enhanced NCW 10.x. Prior to the operational assessment, the Army withdrew 7 of the planned 17 NetOps features because they were not ready for test. The test was conducted in accordance with a DOT&E-approved test plan with the exception of executing adequate manual and instrumented data collection.
- In July 2016, the Army conducted a WIN-T Increment 3 CDT at the contractor's facility. The CDT was designed to demonstrate fixes for NetOps problems discovered during the WIN-T Increment 3 Operational Assessment.
- In September 2016, DOT&E published a WIN-T Increment 3 Operational Assessment report to support a WIN-T Increment 3 AAE decision review.
- In September 2016, the AAE approved the deployment of WIN-T Increment 3 NetOps and NCW enhancements.
- The Army is updating the WIN-T Increment 2 post-full-rate production TEMP to include an FY17 FOT&E to test WIN-T Increment 2 configuration items designed to support light brigades with downsized, air-transportable WIN-T assemblages.

Assessment

- The overall execution of the NIE 16.2 WIN-T Increment 3 Operational Assessment was adequate to support the assessment of operational effectiveness and survivability. It was not adequate to support the assessment of operational suitability due to problems with reliability, availability, and maintainability data collection, documentation of field service representative maintenance activities, and data instrumentation. These problems must be resolved before the next WIN-T operational test event.
- DOT&E assessed the following in the September 2016 WIN-T Increment 3 Operational Assessment report:
  - NCW 10.x enhancements are operationally effective and provide improved support of mission command applications, increased bandwidth and a stable network.
  - Overall, NetOps enhancements were not operationally effective and, due to NetOps and Security Center (NOSC) database failures, did not provide timely and accurate information to NetOps soldiers to conduct their WIN-T network mission. Some NetOps software features – such as the NCW and HNW planning tools – enhanced the soldiers' ability to perform NetOps.
  - Due to complexity, the WIN-T Increment 3 tunnel-less architecture is not effective and adversely affected planning, controlling, monitoring, and visualization at the NOSC.
  - The execution of the NIE 16.2 WIN-T Increment 3 Operational Assessment was not adequate to assess operational suitability.
  - Although survivability has improved, WIN-T Increment 3 still has significant cybersecurity vulnerabilities.
- Following the NIE16.2 WIN-T Increment 3 Operational Assessment, the program took prompt action to resolve NetOps problems identified during operational test. While the July 2016 WIN-T Increment 3 CDT is a good start, none of the tests were of sufficient length and rigor to provide validation of corrective actions.

Recommendations

- Status of Previous Recommendations. The program addressed four of six previous recommendations. They still need to conduct an operational test on WIN-T configuration items designed to support light forces, and improve the integration of WIN-T onto Stryker vehicles.
- FY16 Recommendations. The Army should:
  1. Correct problems with data instrumentation and manual data collection prior to the next WIN-T operational test.
  2. Improve WIN-T cybersecurity and assess its survivability in a future operational test.
  3. Conduct further testing on WIN-T Increment 3 NetOps fixes and validate corrections in a future operational test.
  4. Conduct an operational test to assess WIN-T Increment 2 configuration items designed to support light forces.
  5. Improve Stryker WIN-T integration and demonstrate these improvements in a future operational test.

Navy Programs

Navy Programs

Aegis Modernization Program

Executive Summary

- The Navy is modernizing the Aegis Weapon System (AWS) installed on Baseline 3 USS *Ticonderoga* (CG 47)-class cruisers and Flight I USS *Arleigh Burke* (DDG 51) destroyers to the AWS Advanced Capability Build (ACB)-12 (Baseline 9A and 9C, respectively). New construction Flight IIA DDGs, beginning with USS *John Finn* (DDG 113), will be equipped with Baseline 9C as well.
- Baseline 9A cruiser operational testing began in FY15 and continued through FY16. Baseline 9C destroyer operational testing began in FY16. Neither variant has completed all planned events. In particular, no live-firing events intended to demonstrate surface warfare performance have been executed on any Baseline 9 variant. Additionally, air defense events against supersonic sea-skimming anti-ship cruise missile surrogates have been deferred for reasons including GQM-163A aerial target availability, schedule constraints, and weather.
- In FY16, the SECDEF directed the Navy to fund long-lead items for an Aegis Self-Defense Test Ship (SDTS) to be used for testing of Aegis ACB-20, DDG 51 Flight III, the Air and Missile Defense Radar (AMDR, a.k.a., AN/SPY-6), and Evolved SeaSparrow Missile (ESSM) Block II, and to produce Test and Evaluation Master Plan (TEMP) updates outlining the intended use of the test ship. The Navy has complied with the funding portion of the directive, but has not complied with the remainder of the direction to provide the TEMP or integrated test plan for Aegis ACB-20 and DDG 51 Flight III. Additionally, the Navy has not funded the remainder of the installation/integration cost for the test ship or the remaining test resources to conduct the self-defense testing for ACB-20/DDG 51 Flight III.
- Testing completed to date is insufficient to make a determination of operational effectiveness or suitability for Aegis Baseline 9A or 9C.
- The lack of an adequate modeling and simulation (M&S) suite of the Aegis Combat System (ACS), as well as the lack of an Aegis-equipped SDTS where the ship's full self-defense kill chain can be tested, precludes assessment of the Baseline 9 Probability of Raid Annihilation requirement self-defense mission.
- The Navy will not fully assess Aegis Integrated Air and Missile Defense (IAMD) until a validated M&S test bed is developed and validated. The test bed is planned to be available by FY20, but there is no agreed upon strategy to validate the model to support assessment of the close-in, self-defense battlespace.
- Navy Integrated Fire Control – Counter Air (NIFC-CA) From-the-Sea (FTS) Increment I became a fielded capability in 2015 and fully integrated as a tactical option in fleet air defense. Future testing of the ACB-16 and ACB-20 Aegis Modernizations and Standard Missile-6 (SM-6) will evaluate the NIFC-CA FTS Increment II capability.

System

- The Navy's Aegis Modernization program provides updated technology and systems for existing Aegis-guided missile cruisers and destroyers. This planned, phased program provides similar technology and systems for new construction destroyers.
- The AWS integrates the following components:
  - AWS AN/SPY-1 three-dimensional (range, altitude, and azimuth) multi-function radar
  - AN/SQQ-89 undersea warfare suite that includes the AN/SQS-53 sonar, SQR-19 passive towed sonar array (DDGs 51 through 78, CGs 52 through 73), and the SH-60B or MH-60R helicopter (DDGs 79 Flight IIA and newer have a hangar to allow the ship to carry and maintain its own helicopter)
  - Close-In Weapon System
  - A 5-inch diameter gun
  - Harpoon anti-ship cruise missiles (DDGs 51 through 78, CGs 52 through 73)
  - Vertical Launch System that can launch Tomahawk land attack missiles, Standard surface-to-air missiles, ESSMs, and Vertical Launch Anti-Submarine Rocket missiles
- The Navy is upgrading the AWS on USS *Ticonderoga* (CG 47)-class cruisers and Flight I USS *Arleigh Burke* destroyers to Baseline 9A and 9C, respectfully. Baseline 9 will provide the following new capabilities:
  - Full SM-6 integration
  - IAMD, to include simultaneous air defense and ballistic missile defense missions on Aegis destroyers equipped with the new Multi-Mission Signal Processor
  - NIFC-CA FTS capability

- Starting with USS *John Finn* (DDG 113), the AWS on new construction Aegis-guided missile destroyers is Baseline 9C.

Mission

The Joint Force Commander/Strike Group Commander employs AWS-equipped DDG 51-guided missile destroyers and CG 47-guided missile cruisers to conduct:

- Area and self-defense anti-air warfare in defense of the Strike Group
- Anti-surface warfare and anti-submarine warfare
- Strike warfare, when armed with Tomahawk missiles
- IAMD to include simultaneous offensive and defensive warfare operations
- Operations independently or in concert with Carrier or Expeditionary Strike Groups and with other joint or coalition partners

Major Contractors

- General Dynamics Marine Systems Bath Iron Works – Bath, Maine
- Huntington Ingalls Industries (formerly Northrop Grumman Shipbuilding) – Pascagoula, Mississippi
- Lockheed Martin Maritime Systems and Sensors – Moorestown, New Jersey

---

Activity

- The Navy continued Baseline 9A operational testing in December 2015, but weather and schedule constraints prevented execution of a majority of the planned events. Uncompleted events include a combined surface warfare and air defense firing scenario and a combined supersonic sea-skimming and subsonic sea-skimming anti-ship missile raid. The Navy currently has not re-scheduled these events.
- The Navy began at-sea operational testing of Baseline 9C in March 2016. Two of three planned air defense scenarios were executed, with one of the scenarios executed twice due to execution difficulties. A multi-mission firing scenario combining air defense and surface warfare could not be conducted because of ship system problems and uncooperative weather. Additional surface warfare tracking exercises also remain unexecuted.
- The Baseline 9C testing in March 2016 included operational testing in the undersea warfare area in conjunction with AN/SQQ-89 testing. The undersea warfare testing included exercises against USS *Cheyenne* (SSN 773).
- The Navy planned to conduct Baseline 9C manned aircraft raids in late FY16, but was unable to schedule needed supporting assets. A planned live-firing event including both supersonic and subsonic anti-ship cruise missile surrogates was deferred prior to the start of the March 2016 testing due to GQM-163 aerial target availability.
- Remaining Baseline 9C operational testing, including previously unexecuted events, deferred events, a maintenance demonstration, and cybersecurity testing are planned to occur in FY17.
- The Navy conducted all operational testing in accordance with the DOT&E-approved test plans.
- In February 2016, the SECDEF directed the Navy to acquire long-lead items needed for an Aegis and AMDR SDTS required for conducting adequate self-defense operational testing for DDG 51 Flight III, Aegis ACB-20, AMDR (also known as AN/SPY-6), and ESSM Block II. The Navy complied with this direction by budgeting for a single face of the AMDR to be procured. However, the Navy has not budgeted for the needed Aegis Combat System or the test resources to support the self-defense operational testing for DDG 51 Flight III. The Navy also was directed to update the Aegis/Flight III, AMDR, and ESSM TEMPs, to include the Aegis SDTS and self-defense test events; the Navy has not complied with this direction.
- The Navy is developing an M&S suite that can supplement live testing and facilitate a robust statistical evaluation of air defense performance for DDG 51 Flight III ships after an Aegis-equipped SDTS is available in FY23. As part of the overall M&S development effort, the Navy plans to make limited use of the suite for operational testing of the ACB-16 (Baseline 9C2) in FY22.
- NIFC-CA FTS Increment I became a fielded capability in 2015 after completing developmental testing and is now fully integrated as a tactical option in fleet air defense. Future testing of the ACB-16 and ACB-20 Aegis Modernizations and SM-6 will evaluate the NIFC-CA FTS Increment II capability.
- In September 2016, at White Sands Missile Range, New Mexico, the Navy and Marine Corps successfully conducted a NIFC-CA FTS Increment I demonstration event using an F-35 Lightning II as a targeting source for the Aegis Baseline 9 Desert Ship test configuration and the SM-6. This demonstration was part of developmental testing and did not represent a fleet operational configuration of the ACS or the communications path that would be needed. The demonstration used a non-tactical engineering computer software build in the Aegis Desert Ship test site – itself not fully representative of the ACS – interfaced to a datalink gateway that could receive the F-35 Multifunction Advanced Data Link (MADL) and port track data from the aircraft sensor to the AWS. Using this track data, an SM-6 was initialized and launched at an MQM-107 unmanned target drone.

Assessment

- Baseline 9A and 9C testing completed to date was not sufficient to support an assessment of operational effectiveness or suitability prior the FY15 USS *Normandy* and USS *Benfold* deployments. In accordance with Section 231 of the National Defense Authorization Act for FY08, DOT&E submitted Early Fielding Reports for each baseline. The 12 live flight tests events on Baseline 9A and 9C ships to date suggest that area air defense performance against single subsonic and supersonic high-diving targets is consistent with historical performance against comparable threats, but is not necessarily operationally relevant. The Navy has not yet demonstrated performance against more stressing presentations during operational testing. Operational testing, to include more stressing presentations, is planned to continue through FY17.

- The Navy will not fully assess Aegis IAMD until an AWS M&S test bed is developed and validated. The test bed is under development and is planned to be available by FY20; however, there is no agreed upon strategy to validate the model to support assessment of the close-in, self-defense battlespace. A limited Baseline 9C IAMD operational assessment suggests that DDGs can simultaneously support limited air defense and ballistic missile defense missions, within overall radar resource constraints. This assessment is supported by a single successful live firing event, managed by the Missile Defense Agency, which included simultaneous live firing of SM-2 and SM-3 missiles against threat representative targets in an IAMD engagement.
- Although not presented for operational testing, the Baseline 9A surface warfare performance, specifically to counter high-speed surface threats in littoral waters, as demonstrated during developmental testing, indicated no improvements over previous Aegis baseline operational test results. For both Baseline 9A and 9C, these results indicate that AWS does not fully meet desired surface warfare performance levels.
- As appropriate, and until the full capability may be operationally tested, DOT&E will provide periodic capability assessments to inform Navy and OSD leadership, as well as Congress, on the progress of T&E of the IAMD mission area.
- Until an Aegis-equipped SDTS is available for testing, it is neither possible to characterize the self-defense capabilities of the Aegis cruisers and destroyers, nor possible to accredit an M&S suite to determine if the ships satisfy their Probability of Raid Annihilation requirements.
- The Navy's NIFC-CA FTS Increment I test events conducted to date were sufficient to demonstrate basic capability; however, these demonstrations were not conducted under operationally realistic conditions or against aerial targets representative of modern threats. Additionally, the scenarios conducted were not sufficiently challenging to demonstrate the NIFC-CA FTS requirements defined in the Navy's September 2012 NIFC-CA FTS Testing Capability Definition Letter. DOT&E will assess and report NIFC-CA FTS (Increment II) performance as part of the FY18-23 ACB-16 and ACB-20 Aegis Modernization operational testing and SM-6 FOT&E.
- The Navy's combined Baseline 9 and SM-6 FOT&E test events to date have been successful with no SM-6 integration issues revealed.
- The Navy's Aegis Baseline 9A cybersecurity testing revealed significant problems, which are classified. The nature of these problems is such that they could pose significant risk to the cybersecurity. Details can be found in DOT&E's Early Fielding Report dated July 2015.
- Changes made to the radar software presented unexpected problems during the initial phase of the Aegis cruiser at-sea operational test. The Navy is addressing these problems and remaining cruiser and destroyer operational testing will provide opportunities to confirm these items have been mitigated.
- During both integrated and operational test events, instability of the Aegis operator consoles adversely affected the conduct of test events. The Navy is addressing these problems and remaining cruiser and destroyer operational testing will provide opportunities to confirm these items have been mitigated.
- Aegis Baseline 9C has incorporated software changes to address performance against certain stressing air defense threat presentations; however, these changes proved ineffective during developmental testing.
- The Navy conducted under-sea warfare (USW) testing on Aegis Baseline 9C utilizing USS *Cheyenne* (SSN 773) as a live, reactive threat surrogate. This testing was more operationally realistic than previously reported USW testing that utilized non-reactive threat simulators. Analysis of test results is ongoing. DOT&E will report on USW mission effectiveness in the final Aegis Baseline 9 operational test report.
- In September 2016, at White Sands Missile Range, New Mexico, the Navy and Marine Corps successfully conducted a NIFC-CA FTS Increment I demonstration event using an F-35 Lightning II as a targeting source to allow the ACS (partial) installed at the Desert Ship test facility, WSMR New Mexico, to engage an aerial target with the SM-6. The configuration of the F-35 and the Desert Ship was not operationally representative, nor was the communications path that would be needed replicated for the test. This demonstration was part of developmental testing and did not represent a fleet operational configuration of the ACS. The demonstration used a non-tactical engineering computer software build in the Aegis Desert Ship test site – itself not fully representative of the ACS – interfaced to a datalink gateway that could receive the F-35 MADL and port track data from the aircraft sensor to the AWS. Using this track data, an SM-6 successfully engaged an MQM-107 unmanned target drone. This demonstration was conducted as a proof of concept to show that the NIFC-CA FTS Increment I capability could utilize additional airborne sensors to provide fire control quality data to the AWS. In the context of the event, this objective was met; however, this demonstration should not be construed as an operational capability.

Recommendations

- Status of Previous Recommendations. The Navy has not addressed the following previous recommendations from FY14. The Navy still needs to:
  1. Continue to improve Aegis ships' capability to counter high-speed surface threats in littoral waters.
  2. Synchronize future baseline operational testing and reporting with intended ship-deployment schedules to ensure that testing and reporting are completed prior to deployment.
  3. Provide the necessary funding to support the procurement of an advanced air and missile defense radar and Aegis-equipped SDTS that are needed to support Aegis Modernization, advanced AMDR DDG 51 Flight III, and ESSM Block 2 operational testing.
  4. For Baseline 9A, develop and deploy necessary cybersecurity corrective actions and verify correction with a follow-on operational cybersecurity test.
- FY16 Recommendations. The Navy should:
  1. Complete the planned FOT&E events as detailed in the approved test plan as soon as practical.
  2. Produce an integrated test strategy and capture that in the TEMPs to be approved by DOT&E for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs as soon as possible.
  3. Include planning for NIFC-CA FTS Increment II and NIFC-Collateral (CC) testing in future updates to the Aegis Modernization ACB-16 and ACB-20 and SM-6 TEMPs.

AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) Program

Executive Summary

- The AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) is not operationally suitable and not operationally effective after Block 1 operational testing was prematurely terminated. DOT&E rescinded approval of the Block 1 operational test plan on June 13, 2016, after numerous performance problems were discovered but not corrected, a significant decline below Capability Production Document (CPD) Key System Attribute (KSA) requirements in reliability occurred, and multiple revisions to the software were made causing serious concern over software stability.
- AARGM was previously evaluated as operationally suitable, but not operationally effective due to multiple deficiencies discovered during IOT&E in FY11-12. Reliability problems below CPD requirements were noted during IOT&E, but the subsequent Verification of Correction of Deficiencies resulted in an improving reliability growth curve projection and numbers which met the CPD reliability requirements.
- The Block 1 Upgrade integrated testing was conducted by Navy test squadrons VX-31 and VX-9 beginning in 4QFY14 and ending after DOT&E rescinded approval in 3QFY16.
- The Navy held a Gate 6 Review on August 2, 2016, to determine the way forward for the program. At this review, the operational test community for the AARGM program (VX-9, Commander, Operational Test and Evaluation Force (COTF), and DOT&E) detailed the numerous problems and deficiencies noted affecting weapon accuracy, declining weapon reliability well below the CPD requirements, and software stability concerns after multiple software changes during the Block 1 Upgrade testing. The Program Office stated that they were now meeting all Key Performance Parameters (KPPs) and should be allowed to continue testing. The operational test community acknowledged that the program is meeting KPPs, but pointed out that the weapon system is failing to meet a KSA (reliability) and several other significant CPD requirements, which affect system performance and accuracy and significantly limit effectiveness against many advanced threats and threat counter-anti-radiation missile (ARM) tactics. Moreover, software was being revised and was not stable for operational testing. Software must be stable and fully production representative with numerous new versions used during operational testing. The Navy leadership agreed with the Program Office and directed that testing continue as developmental testing with VX-9, COTF, and DOT&E participating in an assisting role as necessary/desired.
- The Navy intends to release the Block 1 Upgrade software to the fleet in 3QFY17 without completing operational testing and without adequately addressing the numerous performance, reliability, and software stability problems discovered during Block 1 Upgrade testing.
- AARGM Extended Range (ER) is currently based on the Block 1 Upgrade weapon and will require extensive work to correct the accuracy, reliability, and software deficiencies discovered during Block 1 testing.

System

- AARGM supplements the AGM-88B/C High-Speed Anti-Radiation Missile (HARM) and is specifically designed to prosecute targets that stop radiating, executing point-to-point missions against traditional and non traditional air defense systems.
- AARGM uses a new guidance section and a modified HARM control section and fins. The Navy intends to employ AARGM on F/A-18A-F and EA-18G platforms.
- AARGM incorporates digital Anti-Radiation Homing, a GPS, Millimeter Wave guidance, and a Weapon Impact Assessment transmitter.
  - Anti-Radiation Homing improvements include an increased field of view and increased detection range compared to HARM.
  - The GPS allows position accuracy in location and time.
  - The Weapons Impact Assessment capability allows transmission of real-time hit assessment via a national broadcast data system.
  - The Millimeter Wave radar technology allows target discrimination and guidance during the terminal flight phase.
  - The Weapon uses an internal GPS and Inertial Navigation System with mission planning data to establish Missile Impact Zones and Missile Avoidance Zones in an effort to reduce fratricide.

- The Navy intended for the AARGM Block 1 Upgrade (a software-only upgrade) to deliver Full Operational Capability, including Block 0 capability improvements and software changes to provide deferred capability requirements and address deficiencies identified during IOT&E.

Mission

Commanders employ aircraft equipped with AARGM to conduct pre-planned, on-call, and time-sensitive reactive anti-radiation targeting to suppress, degrade, and destroy radio frequency enabled surface-to-air missile defense systems regardless whether the systems continue radiating or shut down.

Major Contractor

Orbital/Alliant Techsystems – Northridge, California

Activity

- In June 2015, DOT&E approved the AARGM FOT&E test plan developed by the Program Office and COTF. The test plan was adequate to address the testing of deferred capabilities and deficiencies discovered during initial developmental test and evaluation and IOT&E.
- The Block 1 Upgrade integrated testing was conducted by Navy test squadrons VX-31 and VX-9 beginning in 4QFY14 and ending after DOT&E rescinded approval in 3QFY16.
- Based on numerous deficiencies discovered during Phase 1 testing and subsequent rounds of testing, significant software updates were required, and an additional integrated test phase was introduced (Phase 1a). Software versions R2.1, R2.2, R2.2.1, R2.2.2, and R2.2.3 were created and delivered during integrated testing to address some of these deficiencies. R2.2.3 is the current version of software for the Block 1 Upgrade.
- The Navy conducted eight live fire test events during Block 1 Upgrade testing. Two of the eight tests have been determined failures, with both impacting the ground significant distances away from their intended targets and having little to no weapons effect on the actual targets. A thorough analysis of the causes of these weapon misses revealed several significant classified problems affecting the accuracy of the weapon. While these problems do not affect KPPs, they do negatively affect weapon performance and accuracy.
- Multiple operational mission failures (OMFs) occurred during the Block 1 Upgrade testing. Four of the nine weapons delivered to China Lake, California, for testing had hardware failures and were returned to the manufacturer. Subsequent testing revealed a much higher number of OMFs than was previously encountered during IOT&E with system-of-system reliability of 20.77 hours Mean Time Between Operational Mission Failure (MTBOMF) as compared to the CPD requirement and KSA of 28.0 hours (Production Threshold and 280.0 hours Production Objective) and a system under test reliability of 31.15 hours MTBOMF as compared to the CPD requirement of 72.0 hours.
- DOT&E rescinded approval of the operational test plan on June 13, 2016, and directed additional measures to restart OT&E to correct the classified problems affecting weapon accuracy.
- DOT&E also directed the Navy to develop an updated live fire test plan that would result in an acceptable level of statistical confidence after two of the eight live fire shots failed. At a minimum, DOT&E believed that 5 more live fire shots, for a total of 13, would be needed to gain the required statistical confidence in the Block 1 Upgrade.
- DOT&E recommended that the Navy develop a plan to improve weapon reliability as weapon reliability during FOT&E was considerably worse than demonstrated in the poor results of IOT&E.
- The Navy appropriated funding for Orbital/Alliant Techsystems to conduct an assessment to identify near term risks of thermal protection properties of the current nose cone and seeker if the rocket motor were redesigned to extend the missile range. If the assessment results are positive, the Navy is considering funding Orbital/Alliant Techsystems to redesign the rocket motor to use with the current Block 1 seeker for an AARGM ER variant.

Assessment

- The FY16 status is assessed as not operationally suitable and not operationally effective due to numerous deficiencies with weapon performance, accuracy, reliability, and software stability revealed during Block 1 Upgrade testing. The details of these deficiencies will be discussed in the forthcoming classified Block 1 Upgrade Operational Test Report.
- Based on IOT&E test data, AARGM was determined to be operationally suitable, but not operationally effective. The details of these deficiencies are discussed in the classified DOT&E IOT&E report published in August 2012.
- The Navy streamlined the Block 1 Upgrade test design and utilized a combined test strategy of developmental and operational testing simultaneously in a prolonged integrated test phase. There was no dedicated developmental testing designed into this test plan. In retrospect and for future AARGM ER testing, a dedicated developmental test phase is necessary for a weapon system software upgrade of this magnitude. This creates a dedicated period of problem discoveries and corrections to take place prior to beginning operational testing with an operationally representative and stable software version and weapon system.
- The discovery of significant problems found during the detailed analysis of the two live fire test shot failures are classified but significantly affect weapon accuracy and performance. The Navy has chosen to accept the problems

without correction because they are not tied to KPPs and will continue with the software release and fielding. These significant problems mean AARGM will not be effective if used to target existing advanced threat surface-to-air missile systems in current and future conflicts using AARGM. Future doctrine is being developed on the faulty premise that AARGM will be able to address these advanced systems, particularly in an Anti-Access and Area Denial (A2AD) environment. The Navy needs to fix the problems discovered during the Block 1 Upgrade FOT&E, or change their future doctrine to reflect the limitations discovered during this failed operational test.

- The Navy is planning on releasing the Block 1 Upgrade to the fleet without adequate operational testing after DOT&E rescinded approval of the test plan and required the Navy to fix several classified problems affecting weapon accuracy and performance and to correct its declining reliability. The Navy decided to continue testing without correcting the majority of these classified deficiencies or addressing the reliability problems. The Block 1 Upgrade only corrects two deferred KPPs from Block 0 and delivers only a small increase in capability while introducing a host of new performance and worsening reliability problems.
- Block 1 Upgrade performance provides limited employment capability against advanced threat surface-to-air radar systems. AARGM ER is currently based on the Block 1 Upgrade technology and will require extensive work to correct the accuracy, reliability, and software deficiencies discovered during Block 1 testing and documented in DOT&E's memo to the Assistant Secretary of the Navy for Research, Development, and Acquisition dated June 13, 2016.

Recommendations

- Status of Previous Recommendations. The Navy addressed all previous recommendations.
- FY16 Recommendations. The Navy should:
  1. Submit an updated operational test plan for DOT&E's approval to correct the accuracy, reliability, and software deficiencies discovered during previous Block 1 testing prior to fleet release. Conduct dedicated developmental testing prior to further operational testing to ensure the operational test asset performance is stable and is production representative.
  2. Assess current and future Navy and Marine Corps doctrine to counter advanced threat surface-to-air missile systems, particularly in an A2AD environment, taking into account the classified problems discovered during previous testing.
  3. Improve seeker performance against advanced threat surface-to-air radar systems prior to investing time, money, and resources in extending the current system's range in an AGM-88E AARGM ER concept.

Amphibious Assault Vehicle (AAV) Survivability Upgrade (AAV-SU)

Executive Summary

- The Amphibious Assault Vehicle (AAV) – Survivability Upgrade (AAV-SU) program initiated prototype build and test planning in FY15. The Marine Corps started test execution in FY16.
  - Ballistic testing of new external armor coupons completed in June 2016. Preliminary results demonstrate specification-level performance against direct and indirect fire threats, but additional testing is required to fully characterize all areas of the crew-occupied space against the expected range of threats.
  - System-level live fire testing to assess the survivability of the AAV-SU and its crew against mines and IEDs began in September 2016 and will be followed by ballistic exploitation testing to further assess all vulnerable areas.
- Operational testing is scheduled to commence in 2QFY17.

System

- The AAV Family of Vehicles is the U.S. Marine Corps' principal amphibious lift system and armored personnel carrier. It is designed to provide combat support, armor-protected firepower, and mobility for a reinforced rifle squad and associated combat equipment for operations on land or at sea.
- After-action reports from Operation Iraqi Freedom highlighted AAV shortfalls in survivability against explosive threats such as landmines and IEDs. These shortfalls limited the employment of AAVs in Iraq after 2007 and precluded employment in Afghanistan.
- The Marines intend for the AAV-SU program to improve force protection against underbelly explosive threats and maintain land and water mobility performance.
  - The survivability upgrades include new external armor, added spall liner, underbelly protection, lower sidewall protection, integrated blast-mitigating seats, and improved fuel tanks.
  - The performance upgrades account for the added weight due to survivability upgrades and include improvements to the powertrain and suspension in order to maintain or increase the vehicle's land and water mobility performance compared to the current vehicle.
- Initial Operational Capability for the AAV-SU is planned for FY19. It will reach Full Operational Capability in FY23 and it must be sustained until at least 2030. The remainder of the legacy AAVs will be phased out as Amphibious Combat Vehicle increments are fielded. The Marine Corps will field AAV-SU vehicles to each of its two active-component Assault Amphibian Battalions, as well as to the Combat Assault Battalion, 3rd Marine Division, and the Combat Assault Company, 3rd Marine Regiment. Additional vehicles will be utilized for training, testing, and supporting the maintenance cycle.

Mission

- Commanders employ Assault Amphibian Battalions to provide task organized forces to transport assault elements, equipment, and supplies ashore; execute ship-to-shore, shore-to-shore, and riverine operations; support breaching of barriers and obstacles; and provide embarked infantry with armor-protected firepower, communication assets, and mobility.
- AAV-SU-equipped units support surface power projection and, if necessary, forcible entry against a defended littoral region.

Major Contractor

- SAIC – McLean, Virgina

Activity

- The Marine Corps conducted armor coupon testing from May to June 2016 in accordance with a DOT&E-approved test plan.
- DOT&E approved the detailed live fire test plan for the AAV-SU Engineering Manufacturing Development (EMD) Phase in April 2016. The plan includes system-level live fire testing scheduled to occur from September through December 2016 followed by ballistic exploitation testing intended to assess targeted damage tolerance of unique and anticipated system design weaknesses (e.g., armor seams).
- Operational testing is scheduled to begin in 2QFY17.

Assessment

- Preliminary analysis of armor coupon testing confirms that the armor is on track to meet its specifications but additional testing is required to fully characterize all areas of the crew-occupied space against the expected range of threats. Due to the lack of sufficient quantity of armor coupons, the Program Office deferred the additional armor characterization to the ballistic exploitation phase of testing. Armor characterization at this stage in the program could complicate design changes if testing reveals significant armor shortfalls.
- Preliminary evaluation of the first underbody event data, conducted against the AAV-SU at the end of FY16, revealed a system design vulnerability that the Program Office is already investigating and addressing. Analysis of all four system-level live fire events is ongoing and will be reported in the FY17 DOT&E LFT&E report.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendation.
  1. The Marine Corps should ensure that enough test assets (e.g., armor coupons) are allocated for the appropriate phases of test for both the AAV-SU and Amphibious Combat Vehicle 1.1 programs.

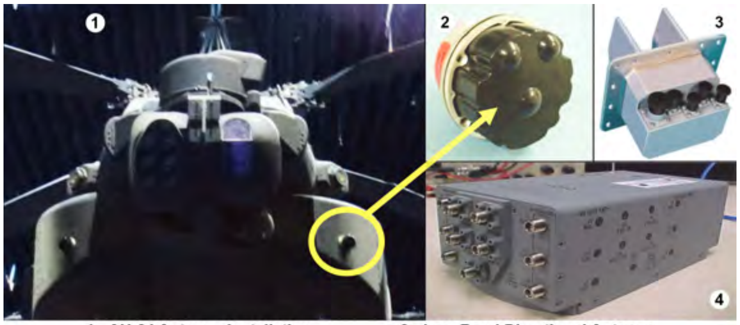
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS)

Executive Summary

- Preliminary results indicate that the AN/APR-39D(V)2 Radar Signal Detection Set (RSDS) has resolved the legacy deficiencies of the AN/APR-39 family (A(V)2, A(V)4, B(V)2, and C(V)2) of Radar Warning Receivers (RWRs).
- Preliminary results indicate an integration problem between the AH 64E platform and AN/APR 39D(V)2 audio warnings. Lack of audio warnings from the AN/APR 39D(V)2, as experienced in developmental test period 2 (DT2), could reduce an aircrew's situational awareness in contested environments.
- Preliminary results indicate the system has a low Mean Time Between Operational Mission Failure (MTBOMF) as tested on the Army's AH 64E platform.

System

- The AN/APR-39D(V)2 is a digital upgrade to the AN/APR-39 family of analog RWRs used by nearly all DOD rotorcraft.
- The AN/APR-39D(V)2 RSDS consists of the following:
  - Four new dual-polarized E through M band (high band) antennas, and a C though D band (low band) direction of arrival antenna.
  - New quadrant receivers (two to four per aircraft). Each receiver has two channels that can accept signals from two E through M band antennas.
  - A new radar data processor with two wideband digital receivers.
  - A crystal video receiver processor and a Quad Core i7 based processor.



1 - AH-64 Antenna Installation
2 - High Band Quadrant Antenna
3 - Low Band Directional Antenna
4 - Quadrant Receiver

- The system uses either a separate display unit or integrates with the onboard aircraft displays to visually and aurally alert the pilots to active threat radars.
- For Navy aircraft, the system also acts as the electronic warfare bus controller.

Mission

Commanders employ units equipped with the AN/APR-39D(V)2 RSDS to improve the mission survivability of Navy and Army aircraft by identifying radio frequency signals from threat surface-to-air missiles, airborne interceptors, and anti-aircraft artillery through cockpit alerts.

Major Contractor

Northrop Grumman – Rolling Meadows, Illinois

Activity

- This is a Navy-led program, but the Army has assumed the test lead due to Navy test aircraft availability problems.
- The Army completed Developmental Test period 1 (DT1) with the AH-64E at the Electronic Combat Range in China Lake, California, in April 2016.
- The Army completed anechoic chamber integrated developmental/operational testing with the AH-64E at the Joint Preflight Integration of Munitions and Electronic Systems facility at Eglin AFB, Florida, in July 2016.
- The Army completed DT2 with the AH 64E at the Electronic Combat Range in October 2016.
- The Army conducted all testing in accordance with the DOT&E-approved test plans.
- The Army completed an operational assessment with the AH-64D and AH-64E at the Electronic Combat Range in November 2016.

Assessment

- Preliminary results indicate that the AN/APR-39D(V)2 RSDS has resolved most of the legacy deficiencies of the AN/APR-39 family of RWRs (A(V)2, A(V)4, B(V)2, and C(V)2).
- Preliminary results indicate an integration problem between the AH-64E platform and AN/APR 39D(V)2 audio warnings. Lack of audio warning from the AN/APR 39D(V)2, as experienced in DT2, could reduce an aircrew's situational awareness in contested environments.
- Preliminary results from laboratory testing indicate that a small number of radar modes could not be detected by the AN/APR-39D(V)2 system. The Navy and Army have requested modifying those symbols to mitigate this limitation.
- Excessive system resets and system degrades occurred during DT1. A reduced number of system resets and system degrades occurred during DT2 as compared with DT1.

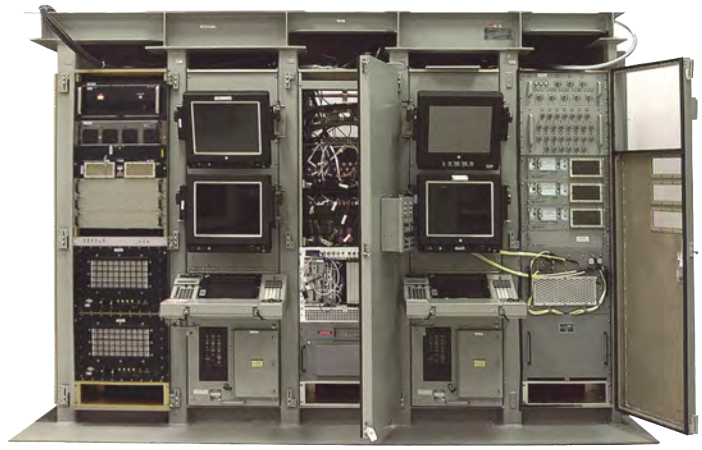
- Preliminary results indicate the system has a low MTBOMF. Testing on the Army's AH-64E platform demonstrated an MTBOMF of 6.7 hours, well below the mission-based derived requirement of 102 hours for the AH-64E and 81 hours for the MV-22B. The Navy intends to fly a KC-130T as a surrogate to accumulate flight hours for system reliability assessment, but available flight hours will not allow demonstration of reliability requirements by the end of FOT&E.
- The system passed all electro-magnetic interference requirements except conductive susceptibility. The system experienced some anomalies for conductive susceptibility during electro-magnetic interference requalification.

Recommendations

- Status of Previous Recommendations. The Navy accomplished all previous recommendations.
- FY16 Recommendations. The Navy and Army should:
  1. Investigate and correct the integration problem related to the lack of AN/APR 39D(V)2 audio warning messages before the Army's AH-64E OT&E in 3QFY17.
  2. Investigate and correct the causes of all system software resets and system degrades.
  3. Incorporate all software and hardware corrections prior to the Navy's anechoic chamber testing with the MV-22 in 2QFY17.
  4. Plan and fly additional KC-130T flights to accumulate more operational flight hours for system reliability assessment.

AN/BLQ-10 Submarine Electronics Warfare Support System

Executive Summary
The Navy conducted an FOT&E of the AN/BLQ-10 system with the Technical Insertion 10 (TI-10) upgrade and the Multifunction Modular Mast (MMM) in August 2016. Analysis of the test results is in progress. DOT&E will provide the final assessment in a 2QFY17 FOT&E Report.



System
- The AN/BLQ-10 system is an electronic warfare support system for U.S. submarines. It provides automatic intercept capability (detection, classification, localization, and identification) for both radar and communications signals. Multiple subsystems process radar and communications signals.
- The AN/BLQ-10 processes signals collected with the submarine's masts. Radar signals are collected by the imaging mast, which is either a photonics mast (on the *Virginia* class) or a periscope (on all other classes). Communications signals are collected from both the imaging mast and a dedicated communications intercept mast, which is either an AN/BRD-7 (on the *Los Angeles* and *Seawolf* classes), an AN/BSD-2 (on the *Virginia* class), or an MMM (recently fielded on some *Los Angeles*- and *Virginia*-class ships). These masts provide largely the same functionality but with different frequency coverage and localization accuracy.
- The program is adopting an open architecture, incremental development process. Hardware and software updates, referred to as a TI, will be fielded every 2 years. TI-08 was the first such upgrade, which added a subsystem to intercept some Low Probability of Intercept (LPI) radar signals.
- The AN/BLQ-10 provides support for specialized, carry-on electronic warfare equipment and personnel.
- TI-10 has been fielded. It consists of updates to commercial off-the-shelf (COTS) processors and displays, as well as upgrades of the Radar Narrowband to improve reliability and maintainability, the addition of Auto Specific Emitter Identification (Auto SEID) to enable automation of the SEID collection processes, and a Nonlinear Resonance Classifier (NRC) upgrade for Improved Communications Acquisition and Direction Finding (ICADF).
- The first TI-14 installations will complete in early FY17, with the first deployment in late FY17 or FY18. It consists of updates to COTS processors and displays, Electronic Warfare Server First Generation, which provides the Electronic Support System operator and platform decision makers with improved tactical situational awareness, and a Radar Rules of Thumb algorithm to provide an assessment of counter detection.

Mission
Submarine Commanders use the AN/BLQ-10 electronic warfare support system to provide threat warning information to avoid counter-detection and collision, and to conduct intelligence, surveillance, and reconnaissance in support of fleet or battlegroup objectives

Major Contractor
Lockheed Martin Mission Systems and Training – Syracuse, New York

Activity
- The Navy:
  - Performed developmental testing on the radar cross section (RCS) of the MMM in June 2015, and released a classified report of the findings in 4QFY15. The Navy conducted additional developmental RCS testing of the MMM in August 2016.
  - Conducted system integration testing in September 2015, to support future developmental tests for TI-14, the next technical insertion release on AN/BLQ-10.
- Commander, Operational Test and Evaluation Force (COTF), the Navy operational test activity:

  - Performed a maintenance demo of AN/BLQ-10 in December 2015 to assess maintainability at the Naval Undersea Warfare Center, Newport, Rhode Island.
  - Conducted an FOT&E of AN/BLQ-10 TI-10 in August 2016 on a *Virginia*-class submarine while underway. This test assessed the improvement in the direction finding abilities of AN/BLQ-10, improvements in the probability of detection and identification of radar emitters, and the integration of the Auto SEID capability. The test was performed in accordance with the DOT&E-approved test plan.

Assessment

- This report provides only a preliminary assessment of the AN/BLQ-10 system with TI-10 based on a June 2015 developmental test report supporting the August 2016 operational test. DOT&E will provide the final assessment in the 2QFY17 FOT&E report after the August 2016 TI-10 operational test data have been analyzed.
- Based on results from the at-sea developmental test in August 2014, there have been no significant changes to communications Direction Finding or radar Direction Finding accuracy from TI-08 to TI-10.
- The addition of the NRC algorithm was intended to reduce workload and improve the performance of ICADF. Initial developmental test results suggest the algorithm has been integrated successfully, but the data analysis of the August 2016 TI-10 operational test must be completed before the operational effectiveness of the system for communications intercept can be assessed.
- Similarly, the performance and functionality of Auto SEID cannot be assessed until the data analysis of the August 2016 TI-10 operational test is complete.
- Several results from previous (TI-08) testing are still applicable to TI-10:
  - The AN/BLQ-10 system is limited in operational effectiveness for some threat radars. The Navy has not yet conducted operational testing against some modern threat radars or appropriate surrogates. The system does detect some radars at long ranges; however, operational testing was inadequate to determine the extent operators can use the AN/BLQ-10 to support submarine missions.
  - The TI-08 upgrade provided improved intercept capability against the intended LPI radars. However, the number of threat LPI radars in the world is increasing and the Navy will need to develop future upgrades to keep up with newer technology.
  - The MMM provides communications localization accuracy that would be sufficient for most submarine missions. TI-08 operational testing showed the system did not meet the Navy's established thresholds.
  - During the TI-08 operational testing, AN/BLQ-10 was not operationally suitable because the Navy's training system was not sufficient to allow fleet operators to maintain proficiency on the system. The Navy has updated their training program, both in classrooms and on individual submarine platforms. While data analysis is not complete, observations taken during the TI-10 operational test did not note any training shortfalls. DOT&E will assess TI-10 suitability once data analysis of the reliability data is completed.

Recommendations

- Status of Previous Recommendations. The Navy has addressed all previous recommendations.
- FY16 Recommendations. As the data analysis is currently ongoing, any future recommendations will be included in the 2QFY17 FOT&E Report.

AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) Sonar

Executive Summary

- DOT&E submitted a classified FOT&E report on the Advanced Processing Build 2011 (APB-11) variant of the AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) sonar system in November 2015.
- The Navy commenced FOT&E on the APB-13 variant of the AN/BQQ-10 A-RCI sonar system with an evaluation of the cybersecurity capability and in-lab comparison testing between APB-11 and APB-13. At-sea operational testing of APB-13 is expected to complete in FY17.

System

- The AN/BQQ-10 A-RCI sonar system is the undersea sensing system utilized by U.S. submarines. It uses active and passive sonar to conduct anti-submarine warfare (ASW) and submerged operations in the execution of all submarine assigned missions. Acoustic energy is processed and displayed to enable operators to detect, classify, localize, and track threat submarines and other waterborne objects (surface ships, mines, bottom features, etc.).
- AN/BQQ-10 A-RCI sonar system is an open architecture system that includes biennial software upgrades (APBs) and quadrennial hardware upgrades (Technology Insertions). These upgrades are intended to maintain an advantage in acoustic detection of threat submarines.
- The AN/BQQ-10 A-RCI sonar system consists of:
  - Interface to submarine acoustic sensors to include the spherical array or large aperture bow array, hull array, wide aperture array, conformal array, high-frequency array, and two towed arrays (i.e., the fat line array consisting of the TB-16 or TB-34, and the thin line array consisting of the TB-23 or TB-29).
  - Processing capability that utilizes environmental data (i.e., water depth, bottom contour, sound velocity profiles, etc.) and received acoustic energy on all acoustic sensors and displays the processed data in a way that supports operator search, detection, classification, and localization/track of contacts of concern or contacts of interest.

Mission

The Operational Commander will employ submarines equipped with the AN/BQQ-10 A-RCI sonar system to:

- Search for, detect, and track submarine and surface vessels in open-ocean and littoral sea environments
- Search for, detect, and avoid mines and other submerged objects
- Covertly conduct intelligence, surveillance, and reconnaissance
- Covertly conduct Naval Special Warfare missions
- Perform under-ice operations

Major Contractor

Lockheed Martin Maritime Systems and Sensors – Manassas, Virginia

Activity

- In November 2015, DOT&E submitted a classified FOT&E report on the APB-11 variant of the AN/BQQ-10 A-RCI sonar system.
- In July 2016, the Navy conducted cybersecurity testing on the APB-13 variant of the AN/BQQ-10 A-RCI sonar system in accordance with a DOT&E-approved test plan.
- In August 2016, the Navy commenced in-lab comparison testing between variants APB-11 and APB-13 of the AN/BQQ-10 A-RCI sonar system using recorded data. Data are being collected during a combined developmental and operational test event in accordance with a DOT&E-approved data collection plan. The Navy will supplement its operational assessment with in-lab comparison testing for environments that are not available for at-sea testing. An operational test of APB-13 at-sea performance will commence in FY17.

Assessment

- In the November 2015 classified FOT&E report, DOT&E determined that the APB-11 variant of the AN/BQQ-10 A-RCI sonar system's overall mission performance remains unchanged from previous assessments and further observed an

improvement in system reliability. The report concluded the following regarding performance:
- For ASW, APB-11 passive sonar capability is effective against older classes of submarines in some environments, but is not effective in all environments or against modern threats. Despite an unchanged overall assessment, APB-11 demonstrated improved operator performance metrics over previous APB variants.
- APB-11 is not effective in supporting operator situational awareness and contact management in areas of high contact density; however, platforms equipped with a Light Weight Wide Aperture Array demonstrated improved performance over previous APB variants.
- APB-11 cybersecurity is not effective and remains unchanged from previous variants.
- APB-11 is operationally suitable.

- Analysis of the APB-13 cybersecurity testing is ongoing and results will be reported in FY17.
- In-lab comparison testing between APB-11 and APB-13 will continue into FY17. DOT&E can make no preliminary assessment due to testing being incomplete.
- Due to the biennial software and quadrennial hardware development cycle, the Navy generates and approves the requirements documents and Test and Evaluation Master Plans in parallel with APB development and installation. As a result, the fleet assumes additional risk, since most operational testing is not completed before the system is initially deployed.

Recommendations

- Status of Previous Recommendations. The Navy made progress in addressing four of five recommendations outlined in DOT&E's classified FOT&E report on APB-11, dated November 12, 2015. Six significant recommendations remain outstanding from previous DOT&E reports. The significant unclassified recommendations are:
  1. Re-evaluate the use of the current time difference between system and operator detection times as the ASW Key Performance Parameter for a more mission-oriented metric to accurately characterize system effectiveness.
  2. Evaluate the covertness of the high-frequency sonar during a future submarine-on-submarine test.
  3. Determine the performance of the AN/BQQ-10 A-RCI sonar system in detecting near surface mines.
  4. Evaluate AN/BQQ-10 A-RCI metrics to improve performance under varying environmental conditions and to focus on earlier and longer range operator detection.
  5. Perform an ASW event against a high-end, diesel-electric, hunter-killer submarine at least with the other APB variants (i.e., APB-11 and again in APB-15) of the AN/BQQ-10 A-RCI sonar system and upon introduction of new wet end sensor or software capabilities improving ASW mission capability.
- FY16 Recommendations. None.

AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite

Executive Summary

- In December 2014, DOT&E submitted a classified Early Fielding Report on the Advanced Capability Build 2011 (ACB-11) variant. The report was submitted due to the installation of the ACB-11 variant on ships that deployed prior to IOT&E. From the data collected, DOT&E concluded the system demonstrated some capability to detect submarines and incoming U.S. torpedoes in deep water.
- Operational testing of the ACB-11 variant of the AN/SQQ-89A(V)15 Integrated Undersea Warfare Combat System Suite began in FY14 and is expected to conclude in FY17. The Navy completed at-sea testing in FY16 and is scheduled to complete the cybersecurity evaluation in FY17.

System

- AN/SQQ-89A(V)15 is the primary undersea warfare system used aboard U.S. Navy surface combatants to locate and engage threat submarines. AN/SQQ-89A(V)15 is an open architecture system that includes staggered biennial software upgrades (ACBs) and biennial hardware upgrades called Technology Insertions.
- AN/SQQ-89A(V)15 uses active and passive sonar to conduct anti-submarine warfare (ASW) search. The acoustic energy received is processed and displayed to enable operators to detect, classify, localize, and track threat submarines.
- AN/SQQ-89A(V)15 uses passive sonar (including acoustic intercept) to provide early warning of threat torpedoes.
- The Navy intends to improve sensor display integration and automation, reduce false alerts, and improve onboard training capability to better support operations within littoral regions against multiple sub-surface threats.
- The system consists of:
  - Acoustic sensors – hull-mounted array, Multi-Function Towed Array (MFTA) TB-37 including a towed acoustic intercept component, calibrated reference hydrophones, helicopter and/or ship-deployed sonobuoys.
  - Functional segments used for processing and displaying active, passive, and environmental data.
  - Interfaces with Aegis Combat System for MK 46 and MK 54 torpedo prosecution using surface vessel torpedo tubes, Vertical Launch Anti-Submarine Rocket, or MH 60R helicopters.
- The system is deployed on a DDG 51 class destroyer or CG 47 class cruiser.

Mission

- Theater Commanders use surface combatants with AN/SQQ-89A(V)15 to locate, monitor, and engage threat submarines.
- Maritime Component Commanders employ surface combatants with AN/SQQ-89A(V)15 as escorts to high-value units to protect against threat submarines during transit. Additionally, they use AN/SQQ-89A(V)15 to conduct area clearance and defense, barrier operations, and ASW support during amphibious assault.
- Unit Commanders use AN/SQQ-89A(V)15 to conduct ASW search, track, engage, and defense.

Major Contractor

Lockheed Martin Mission Systems and Training – Manassas, Virginia

Activity

- In December 2014, DOT&E submitted a classified Early Fielding Report for the ACB-11 variant of AN/SQQ-89A(V)15 Integrated Undersea Warfare Combat System Suite. The report was submitted due to the installation of the ACB-11 variant on ships that deployed prior to IOT&E.
- In September 2015, the Navy completed a formal study that identified capability gaps in currently available torpedo surrogates and presented an analysis of alternatives for specific investments to improve threat emulation ability. The Navy

has since taken the following actions to address the identified capability gaps:
  - The Navy received funding through an FY16 Resource Enhancement Project (REP) proposal and is currently in development of a threat-representative high-speed quiet propulsion system.
  - The Navy submitted an FY17 REP proposal to develop a General Threat Torpedo (GTT) that is intended to expand upon the propulsion system under development and provide representation of threat torpedoes in both acoustic performance and tactical logic.
- The Commander, Operational Test and Evaluation Force continued IOT&E on the ACB-11 variant in March 2016. Testing was conducted in accordance with a DOT&E-approved test plan and included ASW transit search and area search operations using AN/SQQ-89A(V)15 onboard a DDG 51 class destroyer. Testing was conducted in conjunction with an Aegis Baseline 9C operational test event in the Pacific Missile Range Facility Operating Areas. Testing focused on ACB-11 capability to support submarine search in shallow water.
- Remaining ACB-11 operational testing is scheduled for March 2017 and will evaluate ACB-11 cybersecurity effectiveness.
- The Navy is reducing delays to MFTA repair by increasing spare MFTA inventory, implementing processes to expedite MFTA replacement on deployed ships, and investment in shipboard diagnostic capability. The Navy intends to further improve MFTA availability by increasing reliability and pre-placement of spare MFTAs in strategic locations.

Assessment

- The final assessment of ACB-11 is not complete, as testing will continue into FY17. DOT&E's classified Early Fielding Report and additional analysis conducted in FY16 suggest the following regarding performance:
  - The ACB-11 variant demonstrated some capability to localize and support prosecution of a threat submarine.
  - The ACB-11 variant does not meet program performance metrics for torpedo detection as assessed against U.S. exercise torpedoes. The Navy is incorporating system modifications in ACB-15 that are intended to improve torpedo detection capability. ACB-13 was determined to be too far in its development process to incorporate these modifications.
  - The ACB-11 variant is currently not suitable due to low operational availability. ACB-11 software reliability is sufficient; however, significant delay in the repair of MFTA and MFTA handling gear resulted in extended periods of limited system capability. MFTA requires continued monitoring to validate effectiveness of Navy actions towards improving its availability. MFTA is the primary sensor for submarine detection and torpedo alertment.
  - No assessment can be made against the smaller midget and coastal diesel submarines due to the Navy having no test surrogates to represent this prevalent threat.
- A representative threat torpedo surrogate is needed for adequate operational assessment of subsequent variants of AN/SQQ-89A(V)15 with improvement in torpedo alertment. The proposed development of the GTT will address many of the DOT&E concerns and is supported by DOT&E. However, the GTT's capability to support operational testing is further dependent upon future Navy decisions to procure a sufficient quantity of GTTs.
- Analysis of in-water testing and the remaining cybersecurity evaluation are expected to complete in FY17. DOT&E expects to submit an IOT&E report for AN/SQQ-89A(V)15 in FY17.

Recommendations

- Status of Previous Recommendations. The Navy has made some progress on the FY15 recommendations. However, the Navy should still:
  1. Develop and integrate high-fidelity trainers and realistic, in-water test articles to improve training and proficiency of operators in ASW search and track of threat submarines, including midget and coastal diesel submarines.
  2. Revisit system requirements to ensure that funded improvement in subsequent ACBs is supporting Navy objectives for ASW against current and imminent threat submarines.
  3. Address the four classified recommendations listed in the December 2014 Early Fielding Report.
- FY16 Recommendations. The Navy should:
  1. Schedule and complete dedicated IOT&E to assess cybersecurity vulnerabilities.
  2. Acquire sufficient quantity of GTT, when developed, to support evaluation of the next ACB that has modifications effecting torpedo recognition capability (detection and/or classification).

CH-53K – Heavy Lift Replacement Program

Executive Summary

- The CH-53K program has four Engineering Development Model (EDM) aircraft to support integrated developmental and operational flight testing. All four aircraft have been flying in the test program since EDM-4 achieved its first flight on August 31, 2016.
- Additionally, the CH-53K program is using a Ground Test Vehicle (GTV) to qualify key dynamic components and assess aircraft stresses, vibrations, and rotor performance. The GTV is a complete CH-53K that is fully representative of the EDM aircraft. Previous main gear box testing on the GTV revealed gear box failures and required engineering changes to correct deficiencies.
- The CH-53K design is not finalized. Some problems discovered during testing have not been solved by Sikorsky. These include high temperatures in the #2 engine bay, main rotor damper overheating, and #2 engine flameouts. The flameouts are caused by fuel system anomalies, necessitating the use of fuel boost pumps for prevention. Fuel boost pumps are not planned for fielding.
- Live fire tests have fallen behind schedule by 6 to 9 months, due in large part to the failure of an H-53 test fixture at China Lake, California. The test fixture has been rebuilt and live fire tests restarted in December 2016.

System

- The CH-53K is a new-build, fly-by-wire, dual-piloted, three-engine, heavy lift helicopter slated to replace the aging CH-53E. The CH-53K is designed to carry 27,000 pounds of useful payload (three times the CH-53E payload) over a distance of up to 110 nautical miles, climbing from sea level at 103 degrees Fahrenheit to 3,000 feet above mean sea level at 91.5 degrees Fahrenheit.
- The greater lift capability is facilitated by increased engine power (7,500 shaft horsepower versus 4,380 horsepower per engine in the CH-53E) and a composite airframe. This composite airframe is lighter than the CH-53E metal airframe.
- The CH-53K design incorporates the following survivability enhancements:
  - Aircraft Survivability Equipment (ASE) to include Large Aircraft Infrared Countermeasures with the advanced threat warning sensors (combines infrared, laser, and hostile fire functions into a single system), AN/APR 39D(V)2 radar warning receiver, and AN/ALE-47 countermeasure dispensing system
  - Pilot armored seats, cabin armor for the floor and sidewalls, fuel tank inerting, self-sealing fuel bladders, and 30-minute run-dry capable gear boxes
- The Navy intends the CH-53K to maintain a logistics shipboard footprint equivalent to that of the CH-53E.

Mission

- Commanders will employ the Marine Air-Ground Task Force equipped with the CH-53K for:
  - Heavy lift missions, including assault transport of weapons, equipment, supplies, and troops
  - Supporting forward arming and refueling points and rapid ground refueling
  - Assault support in evacuation and maritime special operations
  - Casualty evacuation
  - Recovery of downed aircraft, equipment, and personnel
  - Airborne control for assault support

Major Contractor

Sikorsky Aircraft Corporation (owned by Lockheed Martin since November 2015) – Stratford, Connecticut

Activity

- The program has four EDM aircraft to support integrated developmental and operational flight testing. Sikorsky is manufacturing the first of six system development test article aircraft at its facility in West Palm Beach, Florida; delivery of the first four is projected for FY17.
- All four EDM aircraft have been flying in the integrated test program since EDM-4 achieved first flight on August 31, 2016. The four EDM aircraft have flown 221.2 hours as of October 25, 2016.

- The first operational assessment using Marine Corps pilots and ground personnel completed all ground and flight events at the contractor facility in West Palm Beach, Florida, concluding on October 19, 2016.
- The Navy has used ongoing GTV testing to qualify design changes to key dynamic components and assess aircraft stresses, vibrations, and rotor performance. The GTV is supporting long-term verification and reliability testing. After 72.8 hours of running under representative flight loads, the GTV was torn down for detailed inspection of dynamic components. Inspections revealed no anomalies.
- The GTV will be used for transportability demonstrations on a C-17 airlifter and it will be the test article for full-up system-level LFT&E projected for FY19.
- The pilots' armored seats experienced thermal cracking during initial environmental qualifications and had to be redesigned in FY13. The new design was qualified by analysis and has been part of the qualification program to date. Final environmental and live fire testing of the redesigned pilot seat armor against the specification small arms threat occurred in November 2015.
- In FY15, the Navy completed ballistic testing of four flight-critical main and tail rotor system components. Testing was conducted against a range of operationally relevant small arms threats and under static loads representative of flight conditions. Two of these damaged components were subjected to post-ballistic endurance testing in FY16 to assess the residual flight capability representative of get-home flight and landing conditions. The remaining two components will be tested in FY17.
- In October 2016, the Navy completed live fire testing of the main rotor gear box. Testing was conducted against a range of operationally relevant small arms threats.
- Due to the failure of a test fixture at Naval Air Weapons Station China Lake, California, the live fire testing of two major drive system components, originally scheduled for FY16, was delayed approximately 6 to 9 months. The test fixture has been rebuilt and testing restarted in December 2016.
- Live fire testing of the main and tail rotor servos have been delayed due to problems with arranging testing at the manufacturer's facility in the United Kingdom. Testing of these components has now slipped into FY17.
- The Navy is modifying ASE to address cybersecurity requirements (data at rest protection), mitigate obsolescence (removable media and computer processors), and reduce life cycle cost (elimination of components). The Navy is upgrading the infrared countermeasure subsystem and adding hostile fire indication.
- Due to ASE program delays, the Navy has deferred deployment and testing of the updated ASE and it will not be available for IOT&E. Legacy ASE will be used during IOT&E and will be employed for Initial Operational Capability, which is projected for FY19. Updated ASE will be tested in follow-on tests and retrofitted to the fleet as it becomes available.
- The Navy has continued testing in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and a DOT&E-approved 2010 Alternative LFT&E plan.
- The Program Office is revising the TEMP to reflect programmatic changes and updates to the cybersecurity test strategy for Milestone C to include a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment. Completion of the revised TEMP has slipped into FY17.

Assessment

- Previous main gear box testing on the GTV revealed gear box failures. The required engineering changes and additional testing have contributed to the schedule slip.
- Design of the CH-53K is not finalized. Problems discovered in developmental testing have not been solved.
  - The #2 engine bay is experiencing temperatures high enough to trigger the engine fire light. The contractor has not yet identified a permanent solution.
  - Main rotor dampers are overheating. The contractor has proposed a new rotor damping configuration involving lower damping action, which has been installed on EDM-1. Flight test data are being gathered and analyzed to evaluate the effectiveness of the change.
  - The fuel system configuration has not been finalized in that the original design called for suction-only fuel feed to reduce vulnerability to ballistic threats. When the #2 engine has been run without using a fuel boost pump, prolonged hovering for at least 15 minutes with a 6 degree nose-up attitude has caused the #2 engine to flame out on landing. The contractor has not identified a non-boost pump solution. If boost pumps are required, additional live fire testing may be required.
- Preliminary assessment of the sponson fuel cell qualification test data indicates acceptable performance against small arms threats. Additional live fire ballistic tests will be performed on the GTV in FY19.
- The program successfully completed ballistic qualification testing of the redesigned cockpit armored seats in November 2015. The copilot seat wing armor is being redesigned. This should not invalidate the ballistic results. Once the seat wing armor final design is known, additional qualification testing will be done to evaluate the changes.
- Three of the four flight-critical main and tail rotor system components tested to date demonstrated the required ballistic damage tolerance to the specified projectile. Structural cyclic endurance testing of two of these components in operationally representative conditions has been completed. The Navy will report on any consequent effect of the observed damage on aircraft survivability and fly-home capability in FY17.

Recommendations

- Status of Previous Recommendations. The Navy should continue to address the FY15 recommendations.
  1. Review data resulting from a DOT&E-funded joint live fire program to assess CV-22 armor performance against threats that the Navy did not address in the CV-22 Advanced Ballistic Stopping System LFT&E program. This will enable the Navy to better understand the effectiveness of the similar seats and armor used in CH-53K against additional operationally realistic threats, and to adjust the CH-53K tactics, techniques, and procedures, as needed.
  2. Finish TEMP Revision C, which has slipped from FY16 into FY17.
- FY16 Recommendations. The Navy should
  1. Finalize the CH-53K configuration while remediating problems identified in developmental testing.
  2. Continue testing and finalize the CH-53K design.
  3. Hold Milestone C after the testing has provided confidence in the CH-53K design and data for reliability growth have been collected against the final design.
  4. Consider re-baselining the program to an event-based schedule instead of fixed calendar dates.

Close-in Weapon System (CIWS) – SeaRAM Variant

Executive Summary

- The Navy tested SeaRAM on the Self-Defense Test Ship (SDTS) at the Pacific Test Range, Pt Mugu, California, from December 2015 to March 2016 and on USS *Porter* (DDG 78) at the Spanish sea range, Rota, Spain, in March 2016. None of these tests were conducted with DOT&E-approved operational test plans or conducted by the Navy's Commander, Operational Test and Evaluation Force since SeaRAM is not a formal acquisition program with approved requirements documents or milestone decisions.
- DOT&E published a classified report to Congress in December 2016 since SeaRAM was deployed on operational DDG 51-class ships without having conducted any operational testing. That report stated that, based on the results of the Navy testing, although SeaRAM has demonstrated some capability against anti-ship cruise missile (ASCM) threats, the lack of ASCM surrogate targets to adequately represent advanced ASCM threats combined with the paucity of test data does not support a meaningful and quantitative assessment of SeaRAM's ability to provide the DDG 51 class with an adequate self-defense against threat ASCMs.

System

- SeaRAM is a non-acquisition program that is a standalone self-defense system composed of the Close-in Weapon System (CIWS) radar, an electronic warfare sensor suite, and a modified CIWS command/decision capability combined with an 11-round Rolling Airframe Missile (RAM) launcher (instead of the CIWS 20 mm gun). It provides a short-range, lightweight, self-defense system to defeat ASCMs.
- SeaRAM, as used on selected DDG 51-class ships, can launch the RAM Block 2 that incorporates changes to improve its kinematic capability and its capability to guide on certain types of ASCM radio frequency threat emitters in order to defeat newer classes of ASCM threats

Mission

Commanders of naval surface forces use SeaRAM to provide a short-range, hard-kill engagement capability against ASCM threats for ship self-defense.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- The Navy tested SeaRAM on the SDTS at the Pacific Test Range, Pt Mugu, California, from December 2015 to March 2016, and on USS *Porter* (DDG 78) at the Spanish sea range, Rota, Spain, in March 2016. None of these tests were conducted with DOT&E-approved operational test plans or conducted by the Navy's Commander, Operational Test and Evaluation Force since SeaRAM is not a formal acquisition program with approved requirements documents or milestone decisions.
- DOT&E published a classified Early Fielding Report to Congress in December 2016 since SeaRAM was deployed on operational DDG 51-class ships without having conducted any operational testing.

Assessment

- The classified December 2016 DOT&E report to Congress stated that, based on the results of the Navy testing, although SeaRAM has demonstrated some capability against ASCM threats, the lack of ASCM surrogate targets to adequately represent advanced ASCM threats combined with the paucity of test data does not support a meaningful and quantitative assessment of SeaRAM's ability to provide the DDG 51 class with an adequate self-defense against threat ASCMs.
- An adequate set of DOT&E-approved SeaRAM operational tests against a broader, more threat representative set of ASCM threat surrogates are required to demonstrate that the DDG 51-class destroyer's other defensive weapons do not degrade SeaRAM's effectiveness and to fully assess

SeaRAM's ability to effectively defend DDG 51-class destroyers. Along with additional missile firings, these tests would involve modeling and simulation using an end-to-end model of the DDG 51-class destroyer's combat system that could be accredited for operational testing.

- Further details of SeaRAM's demonstrated capability to provide the DDG 51-class destroyer with an adequate self-defense against threat ASCMs are classified.
- The SeaRAM electronic warfare suite prevents SeaRAM from utilizing the RAM Block 2 missile to its full capability.
- Due to the Navy's inability to develop a Multi-Stage Supersonic Target (MSST), no assessment of SeaRAM's capability against MSST-like ASCM threats is possible.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Navy should:
  1. Plan and program funds for an adequate set of SeaRAM operational tests against a broader set of ASCM threats (to include a phase of modeling and simulation) to fully assess SeaRAM's ability to effectively defend DDG 51-class destroyers. The missile firing portion of these tests could be conducted on an Aegis-equipped SDTS.
  2. Develop threat surrogate aerial targets that adequately represent advanced ASCM threats.
  3. Upgrade the SeaRAM electronic warfare system so that SeaRAM may take full advantage of the RAM Block 2 missile capabilities.
  4. Develop an MSST adequate for use in OT&E. The Test Resources section of this Annual Report provides further details.

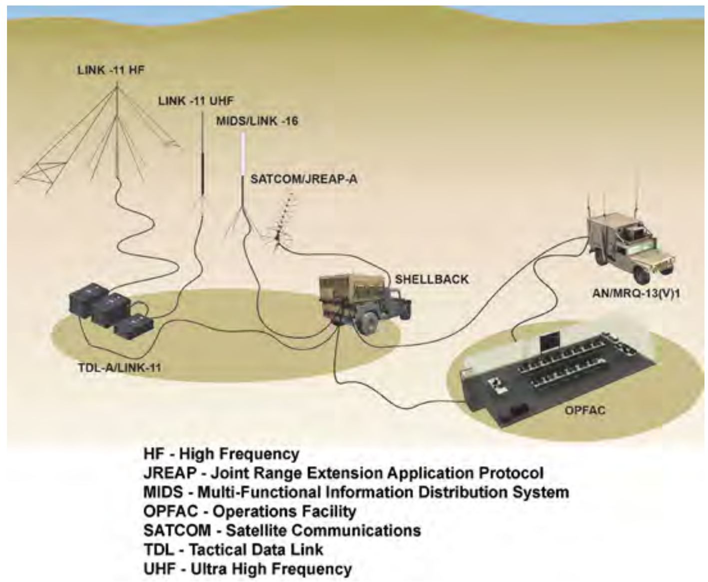
Common Aviation Command and Control System (CAC2S)

Executive Summary

- In 2QFY15, the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN(RD&A)), as the Milestone Decision Authority, conducted a Milestone C review for the Common Aviation Command and Control (C2) System (CAC2S), which resulted in an approval to enter the Production and Deployment Phase of its life cycle and to procure low-rate initial production items to support IOT&E.
- During 3QFY15 and 4QFY15, the Marine Corps conducted additional data fusion testing using updated operational scenarios, and integrated/interoperability testing with the Composite Tracking Network. The Marine Corps continued risk reduction efforts by conducting a full Tactical Air Command Center (TACC) functionality demonstration during a 1QFY16 Weapons and Tactics Instructors' (WTI) exercise at Marine Corps Air Station (MCAS) Yuma, Arizona, as well as conducted datalink testing and an integration demonstration with the Ground/Air Task Oriented Radar (G/ATOR).
- During the 1QFY16 WTI exercise, the Marine Corps continued operational testing of CAC2S using effectiveness and suitability data collected to support the 3QFY16 CAC2S IOT&E.
- In 3QFY16, the Marine Corps Operational Test and Evaluation Activity (MCOTEA) completed the IOT&E for the CAC2S Increment I Phase 2 during the WTI exercise at MCAS Yuma. The IOT&E was conducted in accordance with a DOT&E-approved test plan.
- During the IOT&E, CAC2S demonstrated that it was operationally effective and operationally suitable to support mission accomplishment of the three Marine Corps aviation command and control agencies. Additionally, CAC2S demonstrated the ability to provide data fusion of real-time, near real-time, and non real-time information onto a single tactical display.
- Cybersecurity testing of CAC2S during IOT&E identified significant system vulnerabilities that make it susceptible to compromise in a contested network environment.
- In 4QFY16, Program Executive Officer Land Systems conducted the Fielding Decision Review.

System

- CAC2S consists of tactical shelters, software, and common hardware. The hardware components are expeditionary, common, modular, and scalable. Components may be assembled in a number of configurations to include transportable shelters (via the High Mobility Multi-purpose Wheeled Vehicle), tactical shelters, general-purpose tents, and available military or civilian facilities.



- CAC2S Increment I is being delivered in two phases. Phase I previously delivered hardware and software to fully support the Direct Air Support Center (DASC) mission requirements and partially support Tactical Air Operations Center (TAOC) mission requirements. Phase 2 combines the three legacy Phase 1 systems into two functional subsystems and fully supports the requirements of the DASC, TACC, and TAOC.
  - The Communication Subsystem provides the capability to interface with internal and external communication assets and the means to control their operation.
  - The Aviation Command and Control System provides:
    - The operational command post and functionality to support mission planning, decision making, and execution tools to support all functions of Marine Aviation
    - An open architecture interface capable of integrating emerging active and passive sensor technology for organic and non-organic sensors to the Marine Air Command and Control System
    - The capability to display real-time, near real-time, and non real-time sensor data to support C2 of Marine Air Ground Task Force (MAGTF) aviation assets

Mission

- The MAGTF Commander will employ Marine Corps aviation C2 assets, including the DASC, TAOC, and TACC equipped with CAC2S, to integrate Marine Corps aviation into joint and combined air/ground operations in support of Operational

Maneuver from the Sea, Sustained Operations Ashore, and other expeditionary operations.
- The MAGTF Commander will execute C2 of assigned assets afloat and ashore in a joint, allied, or coalition operational environment by using CAC2S capabilities to:
  - Share mission-critical voice, video, sensor, and C2 data and information to integrate aviation and ground combat planning and operations
  - Display a common, real-time, and near real-time integrated tactical picture with the timeliness and accuracy necessary to facilitate the control of friendly assets and the engagement of threat aircraft and missiles
  - Provide fusion of real-time, near real-time, and non real-time information to support the MAGTF
  - Access theater and national intelligence sources from a multi-function C2 node
  - Standardize Air Tasking Order and Airspace Control Order generation, parsing, interchange, and dissemination throughout the MAGTF and theater forces by using the joint standard for Air Tasking Order interoperability

Major Contractors
- Phase 1
  - Government Integrator: Naval Surface Warfare Center – Crane, Indiana
  - Component Contractor: Raytheon-Solipsys – Fulton, Maryland
- Phase 2
  - Prime Contractor (no Government Integrator): General Dynamics – Scottsdale, Arizona

---

Activity
- In 2QFY15, the ASN(RD&A), as the Milestone Decision Authority, conducted a Milestone C review for CAC2S, which resulted in an approval to procure low-rate initial production items to support IOT&E.
- In 2015, the Marine Corps conducted data fusion testing using an updated and operationally realistic scenario that more adequately stressed the system.
- During the 1QFY16 WTI course, the Program Office and MCOTEA conducted integrated testing of CAC2S for all operations cells within the TACC and also conducted operational endurance testing as risk reduction for the upcoming IOT&E. During this test period, they also conducted an integration demonstration of CAC2S with G/ATOR as a risk reduction effort since the G/ATOR system is still in development. Data collected during the 1QFY16 WTI exercise were used to support the CAC2S IOT&E in accordance with a DOT&E-approved test plan.
- In 2QFY16, MCOTEA conducted cybersecurity testing of CAC2S with a Cooperative Vulnerability and Penetration Assessment at Marine Corps Base Camp Pendleton, California.
- In 3QFY16, MCOTEA conducted an IOT&E of CAC2S during the 3QFY16 WTI exercise at MCAS Yuma, Arizona. During the IOT&E, MCOTEA also conducted a Cooperative Vulnerability and Penetration Assessment, and the Marine Corps Information Assurance Red Team conducted an Adversarial Assessment. DOT&E published a classified CAC2S IOT&E report in August 2016.
- In 4QFY16, the Program Executive Officer Land Systems conducted the Fielding Decision Review.

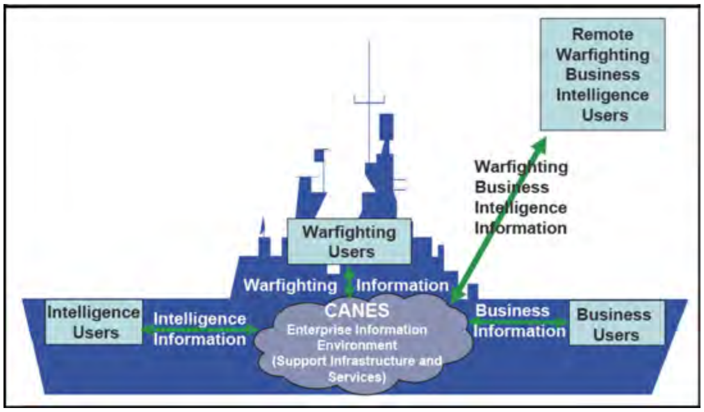
Assessment
- The following assessment is based on quantitative and qualitative evaluation of data from the DT-C2 developmental test period and IOT&E that the Marine Corps conducted during the 1QFY16 and 3QFY16 WTI courses. It is also based on previous data fusion testing. Results are as follows:
  - CAC2S demonstrated that it was both operationally effective and operationally suitable to support the primary mission areas for all three agencies – direct air support for the DASC, control aircraft and missiles for the TAOC, and C2 aviation and planning support for the MAGTF commander in the TACC.
  - CAC2S demonstrated an ability to fuse real-time, near real-time, and non real-time data onto a single tactical display, at low and high operational tempos, and densities of aircraft and targets against current generation threats.
  - DOT&E did observe interoperability/integration of CAC2S with G/ATOR, but since that system is still undergoing development, the Marine Corps will need to conduct an additional evaluation. However, with respect to currently fielded radars (AN/TPS-59) and datalinks, testing successfully demonstrated CAC2S's ability to receive information from those systems displaying both radar plot and track data.
  - Throughout testing, DOT&E observed Tactical Display Framework Chat and Transverse Chat instability as well as problems associated with Voice Laptop freezes. The root causes of these problems were not clear.
  - Reliability, availability, and maintainability data collected during DT-C2 and IOT&E showed CAC2S met its availability and maintainability requirements. CAC2S also met reliability requirements for Mean Time Between Operational Mission Failure but did not meet Mean Time Between Failure requirements during testing. However, Mean Time Between Failure did not affect mission effectiveness as operational availability exceeded the threshold value throughout testing.
  - CAC2S has significant cybersecurity vulnerabilities that make it susceptible to compromise in a contested network

environment. As identified in the classified CAC2S IOT&E report, one cyber-related vulnerability found during penetration assessments should be corrected prior to system fielding.

Recommendations

- Status of Previous Recommendations. The Marine Corps addressed all the previous recommendations.
- FY16 Recommendations. Based on the results of IOT&E and related testing, the Marine Corps should:
  1. Correct cybersecurity vulnerabilities identified in the CAC2S IOT&E report.
  2. Continue data fusion testing of CAC2S with the AN/TPS-80 G/ATOR in FOT&E when G/ATOR becomes available.
  3. Identify root causes and correct Tactical Display Framework Chat and Transverse Chat instability and problems associated with voice laptop freezes. Verify the resolution of both during FOT&E.

Consolidated Afloat Networks and Enterprise Services (CANES)



Executive Summary

- USD(AT&L) approved full deployment of the Consolidated Afloat Networks and Enterprise Services (CANES) on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable. The Commander, Operational Test and Evaluation Force (COTF) conducted IOT&E for the unit-level variant on USS *Higgins* (DDG 76) from August 2014 through March 2015.
- COTF started FOT&E of the force-level CANES variant on the USS *John C. Stennis* (CVN 74) in August 2015. COTF is working to complete the cybersecurity portion of FOT&E without affecting the Navy's mission. COTF expects to conclude cybersecurity operational testing in early 2017.
- The Navy plans to conduct an FOT&E for the submarine variant in FY19.

System

- CANES is an enterprise information system consisting of computing hardware, software, and network services (e.g., phone, email, chat, video teleconferencing, web hosting, file transfer, computational resources, storage, and network configuration and monitoring). CANES will replace legacy networks on ships, submarines, and shore sites.
- The CANES program mitigates hardware and software obsolescence on naval vessels and shore sites through the increased use of standard components and regularly scheduled hardware and software updates.
- The CANES network provides a single, consolidated physical network with logical sub-networks for Unclassified, Secret, Secret Releasable, and Top Secret security domains. It includes a cross-domain solution for information transfers across these security boundaries. This consolidation reduces the network infrastructure footprint on naval platforms and the associated logistics, sustainment, and training costs.
- CANES has three variants tailored to the employing platform: unit level for smaller ships such as destroyers and cruisers, force level for large deck ships such as aircraft carriers and large deck amphibious ships, and a submarine variant.

Mission

Naval Commanders and crew afloat and ashore use CANES to connect weapon systems, host applications, and share command and control, intelligence, and business information via chat, email, voice, and video in support of all naval and joint operations.

Major Contractors

- Northrop Grumman – Herndon, Virginia
- BAE Systems – Rockville, Maryland
- Serco – Reston, Virginia
- DRS Laurel Technologies – Johnstown, Pennsylvania

Activity

- COTF conducted the CANES IOT&E on the unit-level variant from August 2014 through March 2015.
- USD(AT&L) approved CANES full deployment on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable.
- COTF completed the performance and suitability testing portions of FOT&E on the force-level variant aboard USS *John C. Stennis* in August 2015, but could not complete cybersecurity testing at that time because the ship's operational schedule could not support this testing.
- COTF conducted a preliminary Cooperative Vulnerability and Penetration Assessment (CVPA) on USS *John C. Stennis* in December 2015. This test was not intended to satisfy operational testing requirements, but to identify and mitigate as many vulnerabilities as possible before the ship deployed.
- Due to the size and complexity of the force-level CANES, combined with limited ship and Red Team availability, COTF is conducting cybersecurity testing in multiple phases. The first phase focused on embarkable assets (those brought aboard by the destroyer squadron and the ship's air wing). COTF

executed this portion of the test in June 2016 while the ship was underway with the necessary units and assets.

- The test of embarkable assets included both a CVPA and Adversarial Assessment (AA).
- COTF expects to perform a CVPA for the rest of the ship in November 2016 and an AA in March 2017 pending availability of the USS *John C. Stennis* or another suitable test platform.

Assessment

- DOT&E assessed the unit level variant as operationally effective, suitable, and survivable.
- DOT&E will publish an FOT&E report on the CANES force-level variant after the completion of cybersecurity testing in FY17.

Recommendations

- Status of Previous Recommendation. The Navy is addressing the previous recommendation.
- FY16 Recommendations. The Navy should:
  1. Complete the planned cybersecurity tests for force-level ships.
  2. Continue planning the FOT&E for the submarine variant.

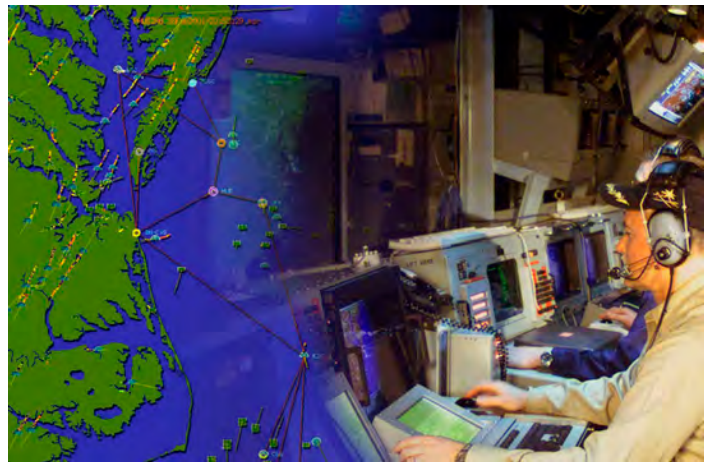
Cooperative Engagement Capability (CEC)

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) continued FOT&E of the Cooperative Engagement Capability (CEC) USG-2B with the Aegis Baseline 9A Combat System in December 2015 and commenced FOT&E of the CEC USG-2B with the Aegis Baseline 9C Combat System in March 2016. Data analysis is ongoing. Preliminary indications are that the CEC USG-2B, as integrated in the Aegis Baseline 9A and 9C Combat Systems, remains operationally effective and suitable and continues to perform comparably to previous CEC USG-2 and USG-2A variants.
- DOT&E will provide a full assessment of the CEC USG-2B's operational effectiveness and suitability on Aegis Baseline 9A and Baseline 9C Combat System platforms upon completion of the CEC USG-2B FOT&Es in late 2017.

System

- CEC is a real-time, sensor-netting system that enables high-quality situational awareness and integrated fire control capability.
- There are four major U.S. Navy variants of CEC:
  - The USG-2/2A is used in selected Aegis cruisers and destroyers, LPD 17/LHD amphibious ships, and CVN 68-class aircraft carriers.
  - The USG-2B, an improved version of the USG-2/2A, is used in selected Aegis cruisers/destroyers as well as selected amphibious assault ships. The USG-2B is planned for use in the CVN 78 and DDG 1000 ship classes.
  - The USG-3 is used in the E-2C Hawkeye 2000 aircraft.
  - The USG-3B is used in the E-2D Advanced Hawkeye aircraft.
- The two major hardware pieces are the Cooperative Engagement Processor, which collects and fuses sensor data, and the Data Distribution System, which exchanges data between participating CEC units.



- The CEC increases Naval Air Defense capabilities by integrating sensors and weapon assets into a single, integrated, real-time network that:
  - Expands the battlespace
  - Enhances situational awareness
  - Increases depth-of-fire
  - Enables longer intercept ranges
  - Improves decision and reaction times

Mission

Naval Commanders use CEC to:

- Improve battle force air and missile defense capabilities by combining data from multiple battle force air search sensors on CEC-equipped units into a single, real-time, composite track picture.
- Provide accurate air and surface threat tracking data to ships equipped with the Ship Self-Defense System.

Major Contractor

Raytheon Systems Co., Command, Control and Communications, Data Systems – St. Petersburg, Florida

Activity

COTF conducted the following CEC test events in FY16 in accordance with the DOT&E-approved test plans:

- Continued FOT&E of the CEC USG-2B with the Aegis Baseline 9A Combat System in December 2015
- Commenced FOT&E of the CEC USG-2B with the Aegis Baseline 9C Combat System in March 2016

Assessment

- CEC test results to date indicate that the CEC USG-2B, as integrated with the Aegis Baseline 9A and 9C Combat Systems, remains operationally effective and suitable and continues to perform comparably to previous CEC USG-2 and CEC USG-2A variants. DOT&E will provide a full assessment of the CEC USG-2B's operational effectiveness

and suitability upon completion of all FOT&Es of Aegis Baselines 9A and 9C with the CEC USG-2B in late 2017.
- Test results indicate that, under certain conditions, some CEC messages were not being distributed to all participating CEC units in the network, resulting in CEC-equipped units having inconsistent tactical pictures which could adversely affect fire control solutions.
- Integration problems were identified during the December 2015 testing when a legacy Aegis baseline ship operated as an assist ship, providing track support to the CEC network. This problem resulted in unnecessary loading of the CEC network. Further details are classified.

Recommendations

- Status of Previous Recommendations. The Navy has not satisfied the following previous recommendations to:
  1. Demonstrate corrections to the problem that degrades the USG-3B CEC's Track File Concurrence in a phase of FOT&E.
  2. Implement changes to the USG-3B CEC interface with the E-2D mission computer that would allow data from the E-2D's APY-9 radar to be used by the USG-3B CEC without first requiring the creation of an E-2D Mission Computer track.
  3. Reassess the USG-3B CEC reliability requirement and whether the logistic supply system can support the demonstrated USG-3B CEC reliability.
  4. Correct the cause of the electromagnetic interference between the USG-3B CEC and the E-2D radar altimeter and demonstrate the corrections in a phase of FOT&E.
  5. Take action on the recommendations contained in DOT&E's classified report to Congress on the CEC USG-3B FOT&E.
  6. Complete the FOT&E of the CEC USG-2B with the Aegis Baseline 9A Combat system
  7. Update the CEC Test and Evaluation Master Plan to include details of:
     - The second phase of the USG-3B FOT&E with the supersonic sea-skimming target scenario
     - FOT&E of corrections made to the CEC USG-3B
     - FOT&E of the CEC USG-2B with the Aegis Baseline 9 Combat System
     - FOT&E of the CEC USG-2B with the DDG 1000 Zumwalt Combat System
     - FOT&E of the CEC USG-2B with the CVN 78 Combat System
     - FOT&E of USG-3B CEC to demonstrate the system's ability to support the E-2D's Theater Air and Missile Defense and Battle Force Command and Control missions
     - The test program supporting the Acceleration of Mid-term Interoperability Improvements Project
- FY16 Recommendations. The Navy should:
  1. Complete the FOT&E of the CEC USG-2B with the Aegis Baseline 9C Combat System.
  2. Investigate and correct the cause of some CEC messages not being consistently distributed to all participating units in the CEC network and demonstrate the correction in a phase of FOT&E.
  3. Investigate and correct the integration problems with legacy Aegis baseline combat systems operating in a CEC network and demonstrate the correction in a phase of FOT&E.

CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) is conducting a DOT&E-approved operational assessment that began in September 2015. The assessment was originally scheduled to end in mid-2016 after CVN 78 completed Builder's Sea Trials and Acceptance Trials, but the slip in CVN 78's delivery date has led to a slip in the completion of the operational assessment.
- DOT&E's assessment of CVN 78 remains consistent with the DOT&E Operational Assessment report submitted in December 2013. Poor or unknown reliability of the newly designed catapults, arresting gear, weapons elevators, and radar, which are all critical for flight operations, could affect CVN 78's ability to generate sorties, make the ship more vulnerable to attack, or create limitations during routine operations. The poor or unknown reliability of these critical subsystems is the most significant risk to CVN 78. Based on current reliability estimates, CVN 78 is unlikely to be able to conduct the type of high-intensity flight operations expected during wartime.
- CVN 78 is unlikely to achieve its Sortie Generation Rate (SGR) (number of aircraft sorties per day) requirement. The threshold requirement is based on unrealistic assumptions including fair weather and unlimited visibility, and that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not affect flight operations. DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the demonstrated performance of the *Nimitz*-class carriers as well as to the SGR requirement.
- The Navy identified an inability to readily electrically isolate Electromagnetic Aircraft Launching System (EMALS) and Advanced Arresting Gear (AAG) components to perform maintenance. This limitation will preclude some types of EMALS and AAG maintenance during flight operations, decreasing their operational availability. The Navy plans to examine system improvements in FY17.
- Previous testing at the EMALS functional demonstration test site at Joint Base McGuire-Dix-Lakehurst, New Jersey, discovered excessive airframe stress during launches of F/A-18E/F and EA-18G with wing-mounted 480-gallon external fuel tanks (EFTs). Similar issues were discovered with 330-gallon EFTs on the F/A-18A-D. Additionally, end-of-stroke dynamics with heavy wing stores were discovered for the F/A-18E/F and EA-18G, which will limit maximum launch speed. These discoveries, until corrected, will preclude the Navy from conducting normal operations of the F/A-18A-F and EA-18G from CVN 78. The Navy plans to correct these problems prior to the end of CVN 78 Post-Shakedown Availability (PSA).
- The Navy continued performance testing of the AAG at a jet car track site at Joint Base McGuire-Dix-Lakehurst, New Jersey. This testing examined the performance of the redesigned arresting gear to meet the system specifications. Runway Arrested Landing Site (RALS) with manned aircraft commenced in 2016 and completed 200 aircraft arrestments as of October 28, 2016 (188 roll-in arrestments and 12 fly-in arrestments). RALS testing supports development of the F/A-18E/F limited envelope Aircraft Recovery Bulletin required for the first arrestments onboard CVN 78.
- The CVN 78 design is intended to reduce manning. As manning requirements have been further developed, analysis indicates the ship is sensitive to manpower fluctuations. Workload estimates for the many new technologies such as catapults, arresting gear, radar, and weapons and aircraft elevators are not well-understood. Some of these concerns have already required redesignation of some berthing areas and may require altering standard manpower strategies to ensure mission accomplishment.
- The CVN 78 combat system for self defense is derived from the combat system on current carriers and is expected to have similar capabilities and limitations. The ship's Dual Band Radar (DBR) is being integrated with the combat system and continues to undergo developmental testing at Wallops Island, Virginia. That testing has uncovered tracking, clutter/false track, track continuity, and engagement support problems typical of those seen in early developmental testing, affecting air traffic control and self-defense operations. The Navy is investigating solutions to these problems, but as ship delivery approaches, the likelihood that these problems will persist into IOT&E increases.
- Funding shortfalls are expected to affect testing of the CVN 78 Integrated Warfare System. In July, the Navy noted that a lack of enterprise funding will result in delays to developmental testing of DBR and the CVN 78 Integrated Warfare System during CVN 78's shakedown period. Ultimately, this will lead

to a 10- to 11-month delay in the ship's Combat System Ship Qualification Trial.
- The development and testing of EMALS, AAG, DBR, and the Integrated Warfare System will continue to drive the *Gerald R. Ford's* timeline as it progresses into OT&E.

System
- The CVN 78 *Gerald R. Ford*-class aircraft carrier program is a new class of nuclear-powered aircraft carriers. It has the same hull form as the CVN 68 *Nimitz* class, but many ship systems, including the nuclear plant and the flight deck, are new.
- The newly designed nuclear power plant is intended to operate at a reduced manning level that is 50 percent of a CVN 68-class ship and produces significantly more electricity. The CVN 78 will incorporate EMALS (electromagnetic, instead of steam-powered catapult launchers) and AAG, and will have a smaller island with a DBR (phased-array radars, which replaces/combines several legacy radars used on current aircraft carriers and serve in air traffic control and ship self-defense).
- The Navy intends for the Integrated Warfare System to be adaptable to technology upgrades and varied missions throughout the ship's projected operating life, including increased self-defense capabilities compared to current aircraft carriers.
- In addition to the self-defense features (hard- and soft-kill), the ship has the following survivability features:
  - Improved protection for magazines and other vital spaces as well as the inclusion of shock hardened systems/components intended to enhance survivability.
  - Various installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from peacetime shipboard fire and flooding casualties and from battle damage incurred during combat.
- The Navy redesigned weapons stowage, handling spaces, and elevators to reduce manning, increase safety, and increase throughput of weapons.
- CVN 78 has design features intended to enhance its ability to launch, recover, and service aircraft, such as a slightly larger flight deck, dedicated weapons handling areas, and an increased number of aircraft refueling stations. The Navy set the SGR requirement for CVN 78 to increase the sortie generation capability of embarked aircraft to 160 sorties per day (12-hour fly day) and to surge to 270 sorties per day (24-hour fly day) as compared to the CVN 68 *Nimitz* class SGR demonstration of 120 sorties per day/240 sorties per 24-hour surge.
- The Consolidated Afloat Networks and Enterprise Services (CANES) program replaces five shipboard legacy network programs to provide a common computing environment for command, control, intelligence, and logistics.
- CVN 78 is intended to support the F-35 and future weapons systems over the expected 50-year ship's lifespan. CVN 78 will include a new Heavy underway replenishment system that will transfer cargo loads of up to 12,000 pounds.
- The Navy intends to achieve CVN 78 Initial Operational Capability in late-FY17 or early-FY18 after successful completion of Post Shakedown Availability and Full Operational Capability in FY21 after successful completion of IOT&E and Type Commander certification.

Mission

Carrier Strike Group Commanders will use the CVN 78 to:
- Conduct power projection and strike warfare missions using embarked aircraft
- Provide force and area protection
- Provide a sea base as both a command and control platform and an air-capable unit

Major Contractor

Huntington Ingalls Industries, Newport News Shipbuilding – Newport News, Virginia

---

Activity

Test Planning
- The CVN 78 *Gerald R. Ford*-class carrier Program Office is revising the Test and Evaluation Master Plan (TEMP) 1610 to align planned developmental tests with corresponding operational test phases and to identify platform-level developmental testing.
- The Navy updated the Post Delivery Test and Trials schedule to incorporate the Full Ship Shock Trial (FSST) as directed by the Deputy Secretary of Defense.
- The Navy is planning for a live test to demonstrate the SGR with six consecutive 12-hour fly days followed by two consecutive 24-hour fly days. DOT&E concurs with this live test approach; however, the Navy plan for extrapolating the 8 days of live results to the 35-day design reference mission on which the SGR requirement is based is yet to be decided.

EMALS
- The Navy is conducting installation and checkout of the EMALS in CVN 78. As of July 2016, 121 dead loads (non-aircraft, weight equivalent sled) and 217 no-load tests have been completed on the bow catapults, and 121 dead loads and 168 no-load tests have been completed on the waist catapults.
- In 2014, testing discovered excessive EMALS holdback release dynamics during F/A-18E/F and EA-18G catapult launches with wing-mounted, 480-gallon EFTs. During test launches, the stress limits of the aircraft were exceeded. Testing also discovered similar problems with 330-gallon

EFTs and with end-of-stroke dynamics that affect heavy wing stores. The program has developed fixes, but testing to verify the fixes on manned aircraft has been delayed until 2017 on F/A-18E/F and EA-18G and until 2018 for F/A-18A/B/C/D.

AAG

- The Navy is conducting installation and checkout of the AAG in CVN 78.
- The Navy continues to test the AAG on a jet car track at Joint Base McGuire-Dix-Lakehurst, New Jersey. Earlier testing prompted system design changes that are now being tested. The jet car track testing examined the F/A-18E/F performance envelope with the new design. Overall, land-based jet car track testing has conducted a total of 1,381 dead load arrestments as of November 2016. Testing in 2016 examined degraded mode performance for the safe recovery of aircraft in the event of an AAG component failure. Testing began at RALS to develop the limited envelope Aircraft Recovery Bulletin needed for the first at-sea arrestments on CVN 78.

CANES

- The Navy completed the performance and suitability portions of the CANES follow-on operational testing of the force-level CANES configuration used on the *Nimitz* and *Ford* classes. The cybersecurity testing of this variant is expected to conclude in 2017.
- USD(AT&L) approved full deployment of CANES on October 13, 2015, based on the results of the IOT&E for the unit-level variant conducted from August 2014 through March 2015.

DBR

- The radar consists of fixed array antennas both in the X- and S-bands. The X-band radar is the Multi-Function Radar (MFR) and the S-band radar is the Volume Search Radar (VSR).
- The Navy is testing a production array MFR and an Engineering Development Model array of the VSR at the Surface Combat System Center at Wallops Island, Virginia. Integration testing of DBR continues at Wallops Island and is expected to continue through 4QFY17. The MFR will then be installed on the Self-Defense Test Ship (SDTS) for further CVN 78 testing.
- Limited testing of the production DBR has begun on CVN 78 in the shipyard. While the program has completed over 80 percent of industrial testing, the DBR cannot be fully tested without going to sea and safety precautions within the shipyard limit the extent of testing conducted to date.

Electric Plant

- The newly designed medium-voltage electrical distribution system was initially energized in 2013. Shipboard testing earlier this year, directed by Naval Sea Systems Command (NAVSEA), demonstrated high-power operation of the power generation components using reactor-power generated steam, including support of large electric loads (e.g., EMALS). During recent NAVSEA shipboard testing, an instrumentation transformer associated with the system's main turbine generators voltage regulating system failed. Detailed investigation into this problem indicated that the specific failure was most likely due to a manufacturing defect, but investigation of that original transformer defect continues. To address this component failure and keep the ship on schedule, an alternate design transformer (proven in other electrical applications) was installed but the new configuration was not tested at the land-based test facility to the same degree as the original transformer. Shipboard testing following installation of the alternative transformer revealed design vulnerabilities with the new transformers that must be addressed prior to ship delivery. Voltage regulating system design changes are being implemented and detailed repair plans are in place to address these problems.

Manning

- CVN 78 has been manned in the shipyard, and the Navy is working with the ship's personnel to refine manpower, personnel, training, and education planning.

LFT&E

- The Navy is making progress for executing the Shock Trial on CVN 78 in FY19. The Navy has held internal meetings to discuss shock trial logistics, environmental requirements, and the way forward regarding component shock qualification of mission critical systems.

Assessment

Test Planning

- A TEMP 1610 revision is under development to address problems with the currently-approved TEMP 1610, Revision B. The Program Office is in the process of refining the post-delivery schedule to further integrate testing and to include the FSST.
- The Navy has not finalized how it intends to extrapolate the live SGR testing (six consecutive 12-hour fly days followed by two consecutive 24-hour fly days) to the 35-day design reference mission on which the SGR requirement is based. COTF is working with the Program Office to identify required upgrades for the Seabasing/Seastrike Aviation Model to perform this analysis.
- The schedule to deliver the ship has slipped to December 2016 "under review," meaning the Navy is currently evaluating the power plant problems and repair timeline and is determining a new date for delivery. This new date is planned to be announced in mid-December 2016. Further slips in the delivery are likely to affect schedules for the first at-sea OT&E of CVN 78. Currently, the Program Office is planning for two phases of initial operational testing. The first phase examines basic ship functionality as the ship prepares for flight operations; the second phase focuses on flight operations once the ship and crew are ready. The Navy plans to begin the first phase of testing in late FY18 or early FY19 before CVN 78's FSST. The FSST is followed by CVN 78's first Planned Incremental Availability (PIA), an extended

maintenance period. The Navy then plans to complete the second phase of operational testing after the PIA in FY21, subsequent to when the ship would first deploy. To save resources and lower test costs, the test phases are aligned with standard carrier training periods as CVN 78 prepares for its first deployment. Further delays in the ship delivery are likely to push both phases of testing until after the PIA. As noted in previous annual reports, the CVN 78 test schedule has been aggressive, and the development and testing of EMALS, AAG, DBR, and the Integrated Warfare System are driving the ship's schedule independent of the requirement to conduct the FSST. Continued delays in the ship's delivery will compress the ship's schedule and are likely to have ripple effects. Given all of the above, it is clear that the need to conduct the FSST is not a key factor driving the first deployment to occur in FY21.

Reliability

- CVN 78 includes several systems that are new to aircraft carriers; four of these systems stand out as being critical to flight operations: EMALS, AAG, DBR, and the Advanced Weapons Elevators (AWEs). Overall, the poor reliability demonstrated by AAG and EMALS and the uncertain reliability of DBR and AWEs pose the most significant risk to the CVN 78 IOT&E. All four of these systems are being tested for the first time in their shipboard configurations aboard CVN 78. The Program Office provided updates on the reliability of these systems in April 2016. Reliability estimates derived from test data for EMALS and AAG are discussed below. For DBR and AWE, only engineering reliability estimates have been provided to date.

EMALS

- EMALS testing to date has demonstrated that EMALS should be able to launch aircraft planned for CVN 78's air wing. However, present limitations on F/A-18E/F and EA-tim18G configurations, as well as the system's demonstrated poor reliability during developmental testing, suggest operational difficulties lie ahead for meeting requirements and in achieving success in combat.
- With the current limitations on EMALS for launching the F/A 18E/F and EA-18G in operational configurations (e.g., wing-mounted 480-gallon EFTs and heavy wing stores), CVN 78 will be able to fly F/A-18E/F and EA-18G, but not in configurations required for normal operations. Presently, these problems substantially reduce the operational effectiveness of F/A-18E/F and EA-18G flying combat missions from CVN 78. The Navy has developed fixes to correct these problems, but testing with manned aircraft to verify the fixes has been postponed to 2017.
- As of April 2016, the program estimates that EMALS has approximately 400 Mean Cycles Between Critical Failure (MCBCF) in the shipboard configuration, where a cycle represents the launch of one aircraft. While this estimate is above the rebaselined reliability growth curve, the rebaselined curve is well below the requirement of 4,166 MCBCF. At the current reliability, EMALS has a 7 percent chance of completing the 4-day surge and a 67 percent chance of completing a day of sustained operations as defined in the design reference mission. Absent a major redesign, EMALS is unlikely to support high-intensity operations expected in combat.
- The reliability concerns are exacerbated by the fact that the crew cannot readily electrically isolate EMALS components during flight operations due to the shared nature of the Energy Storage Groups and Power Conversion Subsystem inverters onboard CVN 78. The process for electrically isolating equipment is time-consuming; spinning down the EMALS motor/generators takes 1.5 hours by itself. The inability to readily electrically isolate equipment precludes EMALS maintenance during flight operations, reducing the system's operational availability.

AAG

- Testing to date has demonstrated that AAG should be able to recover aircraft planned for the CVN 78 air wing, but the poor reliability demonstrated to date suggests AAG will have trouble meeting operational requirements.
- The Program Office redesigned major components that did not meet system specifications during land-based testing. In April 2016, the Program Office estimated that the redesigned AAG had a reliability of approximately 25 Mean Cycles Between Operational Mission Failure (MCBOMF) in the shipboard configuration, where a cycle represents the recovery of one aircraft. This reliability estimate is well below the rebaselined reliability growth curve and well below the requirement of 16,500 MCBOMF specified in the requirements documents. At the current reliability, AAG has an infinitesimal chance of completing the 4-day surge and less than a 0.2 percent chance of completing a day of sustained operations as defined in the design reference mission. Without a major redesign, AAG is unlikely to support high intensity operations expected in combat.
- The reliability concerns are worsened by the current AAG design that does not allow Power Conditioning Subsystem equipment to be electrically isolated from high power buses, limiting corrective maintenance on below-deck equipment during flight operations. This reduces the operational availability of the system.

DBR

- Previous testing of Navy combat systems similar to CVN 78's revealed numerous integration problems that degrade the performance of the Integrated Warfare System. Many of these problems are expected to exist on CVN 78. The DBR testing at Wallops Island is typical of early developmental testing with the system still in the problem discovery phase. Current results reveal problems with tracking and supporting missiles in flight, excessive numbers of clutter/ false tracks, and track continuity concerns. The Navy recently extended DBR testing at Wallops Island until 4QFY17; however, more test-analyze-fix cycles are likely to be needed to develop and test DBR fixes so that the DBR can properly perform air traffic control and engagement support on CVN 78.

- Currently, the Navy has only engineering analysis of DBR reliability. The reliability of the production VSR equipment in the shipboard DBR system has not been assessed. While the Engineering Development Model (EDM) VSR being tested at Wallops Island has experienced failures, it is not certain whether these EDM VSR failure modes will persist during shipboard testing of the production VSR. Reliability data collection will continue at Wallops Island and during DBR operations onboard CVN 78. The Navy has identified funding shortfalls that are likely to delay important developmental testing of DBR and the Integrated Warfare System. Test delays are likely to affect CVN 78's readiness for IOT&E. Delays in the development and testing of these systems at Wallops Island have significantly compressed the schedule for self-defense testing of DDG 1000 and CVN 78 on the SDTS. This testing is essential for understanding these ships' capabilities to defend themselves and prevail in combat. The completion of self-defense testing for CVN 78, and the subsequent use of Probability of Raid Annihilation test bed for assessing CVN 78 self-defense performance, are dependent upon future Navy decisions that could include canceling MFR component-level shock qualification or deferring the availability of the SDTS MFR for installation on DDG 1002.

SGR

- CVN 78 is unlikely to achieve its SGR requirement. The target threshold is based on unrealistic assumptions including fair weather and unlimited visibility, and that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not affect flight operations. DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the SGR requirement as well as to the demonstrated performance of the *Nimitz*-class carriers.
- During the 2013 operational assessment, DOT&E conducted an analysis of past aircraft carrier operations in major conflicts. The analysis concludes that the CVN 78 SGR requirement is well above historical levels and that CVN 78 is unlikely to achieve that requirement.
- There are also concerns with the reliability of key systems that support sortie generation on CVN 78. Poor reliability of these critical systems could cause a cascading series of delays during flight operations that would affect CVN 78's ability to generate sorties, make the ship more vulnerable to attack, or create limitations during routine operations. DOT&E assesses the poor or unknown reliability of these critical subsystems will be the most significant risk to CVN 78's successful completion of IOT&E. The analysis also considered the operational implications of a shortfall and concluded that as long as CVN 78 is able to generate sorties comparable to *Nimitz*-class carriers, the operational capabilities of CVN 78 will be similar to that of a *Nimitz*-class carrier.

Electric Plant

- A full-scale qualification unit of the shipboard component was manufactured and tested in a land-based facility in 2004. This test revealed no problems with the design of the original transformers or any other part of the main turbine generator. The design issues revealed during troubleshooting of the failed main turbine generator voltage regulating system transformer were introduced with the design changes incorporated following the transformer failure. Once alternate transformers were selected, the Navy did not perform sufficient land-based testing to validate that no system design flaws or vulnerabilities with the revised voltage regulating system design existed. The Navy considered the risk was low and did not want to further delay ship delivery for the testing. However, due to the failure, ship delivery continues to be delayed.

Manning

- Based on earlier Navy analysis of manning and the Navy's early experience with CVN 78, several areas of concern have been identified. The Navy is working with the ship's crew to resolve these problems.
- During some exercises, the berthing capacity for officers and enlisted will be exceeded, requiring the number of evaluators to be limited or the timeframe to conduct the training to be lengthened. This shortfall in berthing is further exacerbated by the 246 officer and enlisted billets (roughly 10 percent of the crew) identified in the Manning War Game III as requiring a face-to-face turnover. These turnovers will not all happen at one time, but will require heavy oversight and will limit the amount of turnover that can be accomplished at sea and especially during evaluation periods.
- Manning must be supported at the 100 percent level, although this is not the Navy's standard practice on other ships and the Navy's personnel and training systems may not be able to support 100 percent manning. The ship is extremely sensitive to manpower fluctuations. Workload estimates for the many new technologies such as catapults, arresting gear, radar, and weapons and aircraft elevators are not yet well-understood. Finally, the Navy is considering placing the ship's seven computer networks under a single department. Network management and the correct manning to facilitate continued operations is a concern for a network that is more complex than historically seen on Navy ships.

LFT&E

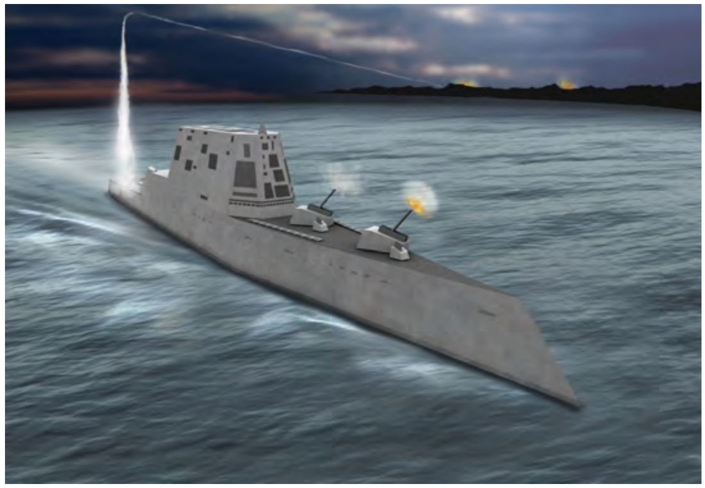
- CVN 78 has many new critical systems, such as EMALS, AAG, AWE, and DBR that have not undergone shock trials on other platforms. Unlike past tests on other new classes of ships with legacy systems, the performance of CVN 78's new critical systems is unknown. Inclusion of data from shock trials early in a program has been an essential component of building survivable ships. The current state of modeling and component-level testing are not adequate to identify the myriad problems that have been revealed only through full ship shock testing. DOT&E has requested that the Navy provide the status of the programs component shock qualification at a minimum on a semi-annual basis to understand the vulnerability and recoverability of the ship.

Recommendations

- Status of Previous Recommendations. The Navy should continue to address the nine remaining FY10, FY11, FY13, FY14, and FY15 recommendations.
  1. Finalize plans that address CVN 78 Integrated Warfare System engineering and ship's self-defense system discrepancies prior to the start of IOT&E.
  2. Provide scheduling, funding, and execution plans to DOT&E for the live SGR test event during the IOT&E.
  3. Continue to work with the Navy's Bureau of Personnel to achieve adequate depth and breadth of required personnel to sufficiently meet Navy Enlisted Classification fit/fill manning requirements of CVN 78.
  4. Conduct system-of0systems developmental testing to preclude discovery of deficiencies during IOT&E.
  5. Address the uncertain reliability of EMALS, AAG, DBR, and AWE. These systems are critical to CVN 78 flight operations, and are the largest risk to the program.
  6. Aggressively fund and address a solution for the excessive EMALS holdback release dynamics during F/A-18E/F and EA-18G catapult launches with wing-mounted 480-gallon EFTs.
  7. Begin tracking and reporting on a quarterly basis systems reliability for all new systems, but at a minimum for EMALS, AAG, DBR, and AWE.
  8. The Navy should ensure the continued funding for component shock qualification of both government- and contractor-furnished equipment.
  9. Submit a TEMP for review and approval by DOT&E incorporating the Deputy Secretary's direction to conduct the FSST before CVN 78's first deployment.
- FY16 Recommendations. The Navy should:
  1. Ensure adequate funding of DBR and Integrated Warfare System developmental testing to minimize delays to the test schedule.
  2. Provide DOT&E with component shock qualification program updates at a minimum of semi-annually, and maintain DOT&E's awareness of FY19 shock trial planning.

DDG 1000 *Zumwalt* Class Destroyer

Executive Summary



- The first ship in the *Zumwalt* class of destroyers was launched on October 28, 2013. The Navy accepted delivery of DDG 1000 in an incomplete condition. In September 2016, the ship set sail for the west coast in order to begin, upon arrival, an 18-month post-delivery availability to complete installation, integration, and shipyard testing of its combat systems. The Navy plans to conduct a second Acceptance Trial when that availability has been completed and expects IOT&E to commence in 3QFY18.
- The Navy is concerned with the high cost of projectiles for the Long Range Land Attack Projectile (LRLAP) for the DDG 1000 Advanced Gun System (AGS) and has not funded LRLAP rounds required to evaluate AGS performance during IOT&E. Without these projectiles, the destroyers' primary mission capability of land attack will be limited to strike with Tomahawk Land Attack Missiles (TLAMs) until a replacement land attack projectile is identified and the AGS is modified to fire the new projectile.
- The roles and missions of DDG 1000 are under review. The Navy expects to complete a study to determine the concept of operations for DDG 1000 by 2QFY17.
- The Navy has requested funding in FY18/19 to execute a reduced scope component shock qualification program, and is going through the process to identify the equipment/systems and shock grade to which these will be qualified.
  - Indications are that the number of components undergoing shock qualification will be a reduced set, which will introduce risk for the shock trial. Additionally, by reducing the number of components undergoing shock qualification, the assessment of the vulnerability and recoverability capability of the ship at design levels for underwater threats will be limited. The Navy had indicated in prior years that the component shock testing would be funded and conducted prior to installation of any equipment on the first ship, which is the normal, common-sense approach. However, the Navy diverted that funding to other uses; thus, the component shock testing was not done and now cannot be done in the normal sequence.
  - Despite these limitations, the shock trials currently scheduled for FY20 must be performed at the traditional severity levels for a surface combatant. These trials will now be the sole source of comprehensive data on the survivability of mission-critical ship systems to shock, and are therefore critical to the success in combat of the ship and her crew.
- Additional AN/SPY-3 multi-function (X-band) radar development and testing at the Wallops Island test facility has significantly compressed the schedule for self-defense testing of both the *Zumwalt*-class destroyer and the CVN 78 *Gerald R. Ford*-class nuclear aircraft carrier on the Navy's self-defense test ship (SDTS). The completion of this live-fire testing, and the subsequent use of the Probability of Raid Annihilation test bed, is essential to be able to evaluate the self-defense and survivability of the *Zumwalt*-class destroyer. The Navy must identify how the required ship self-defense testing will be completed prior to deployment of a *Zumwalt*-class destroyer. This may mean delaying the AN/SPY-3 radar installation on DDG 1002.

System

The *Zumwalt*-class destroyers are new surface combatants with a wave-piercing tumblehome hull form designed both for endurance and low-radar detectability. The Navy currently plans to acquire three ships of the class. The *Zumwalt*-class destroyer is equipped with the following:

- Total Ship Computing Environment Infrastructure that hosts all ship functions on an integrated and distributed computing plant.
- Two 155 mm AGS designed to fire LRLAPs.
- AN/SPY-3 Multi-Function (X-band) radar modified to include a volume search capability. (The Navy removed the Volume Search Radar (S-band) from the ship's baseline design for cost reduction in compliance with an Acquisition Decision Memorandum of June 1, 2010.)
- Eighty vertical launch cells that can hold a mix of TLAMs, Standard Missiles, Vertical Launch Anti-Submarine Rockets, and Evolved SeaSparrow Missiles.
- An integrated undersea warfare system with a dual frequency bow-mounted sonar and multi-function towed array sonar to detect submarines and assist in avoiding in-volume mines.

- Two MK 46 30 mm close-in gun systems for self-defense against small boat swarms. The MK 46 30 mm close-in gun system replaces the MK 110 57 mm close-in gun system. (Configuration change resulted from a Gate 6 Configuration Steering Board of June 2012.)
- An ability to embark and maintain MH-60R helicopters and vertical take-off unmanned aerial vehicles.
- An Integrated Power System that can direct electrical power to propulsion motors, combat systems, or other ship needs.
- In addition to the self-defense features installed on the ship (hard and soft kill), the following survivability features are included in the design:
  - Improved ballistic protection for magazines and other vital compartments and shock hardened systems/components
  - Installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from peacetime shipboard fire and flooding casualties, and from damage incurred during combat
  - Tele-robotic fire nozzles that cover selected areas of the ship

Mission

- The Joint Force Maritime Component Commander intends to employ *Zumwalt*-class destroyers to provide:
  - Joint surface strike/power projection
  - Joint surface fire support
  - Surface warfare
  - Anti-air warfare
  - Anti-submarine warfare
- The Navy expects *Zumwalt*-class destroyers to operate independently or in conjunction with an Expeditionary or Carrier Strike Group, as well as with other joint or coalition partners in a Combined Expeditionary Force environment.

Major Contractors

- General Dynamics Marine Systems Bath Iron Works – Bath, Maine
- Huntington Ingalls Industries – Pascagoula, Mississippi
- BAE Systems – Minneapolis, Minnesota
- Raytheon – Waltham, Massachusetts

Activity

- In September 2015, the Navy completed a formal study that identified capability gaps in currently available torpedo surrogates and presented an analysis of alternatives for specific investments to improve threat emulation ability. The Navy has since taken the following actions to address the identified capability gaps:
  - The Navy received approximately $1.0 Million through an FY16 Resource Enhancement Project (REP) proposal and is currently in development of a threat-representative high-speed quiet propulsion system.
  - The Navy submitted an FY17 REP proposal for $6.2 Million to develop a General Threat Torpedo (GTT) that will expand upon the propulsion system under development and provide representation of threat torpedoes in both acoustic performance and tactical logic.
- In June 2016, the Navy elected to delay installation of the AN/SPY-3 radar on the Navy's SDTS in order to conduct additional development and testing of the AN/SPY-3 radar at the Wallops Island test facility. The AN/SPY-3 array at the Wallops Island test facility is used for system development and testing of the radar systems of both the *Zumwalt*-class destroyer and the CVN 78 *Gerald R. Ford*-class nuclear aircraft carrier. Further, the same AN/SPY-3 array will ultimately be installed on the DDG 1002.
- The Navy ceased planning for live fire events using LRLAP due to concern with the high cost of projectiles for the LRLAP for the DDG 1000 AGS. The Navy continued planning for structural firings and reliability testing of AGS on DDG 1000 using inert firing shapes. The Navy is investigating options to replace the LRLAP land attack capability.
- The roles and missions of DDG 1000 are under review. The Navy expects to complete a study to determine the concept of operations for DDG 1000 by 2QFY17.
- The Navy revised the Test and Evaluation Master Plan (TEMP) and is currently routing it within the Navy for approval.
- The Navy continued development of the DDG 1000 Probability of Raid Annihilation test bed. The test bed is a high-fidelity modeling and simulation (M&S) tool that will be used, in conjunction with live fire testing conducted aboard DDG 1000 and the SDTS to assess *Zumwalt*-class destroyers' capability to defeat hostile anti-ship cruise missiles and aircraft.
- In October 2015, the SECDEF directed the Navy to conduct the *Zumwalt*-class destroyers shock trial prior to the first deployment of any ship of the class. The Navy is developing a plan of action to shock qualify a limited amount of equipment prior to the shock trial to ensure the trial can be safely conducted. The focus of the reduced effort will be on shock qualifying equipment that is critical to personnel safety prior to conducting the shock trial; it is unclear how much of the mission-critical equipment (hull; mechanical; electrical; and command, control, communications, computers, combat systems, and intelligence) will be shock qualified and to what level.

Assessment

- The threat torpedo surrogates currently available for operational assessment of the *Zumwalt*-class destroyer have significant limitations in their representation of threat

torpedoes. The proposed development of a GTT addresses many of the DOT&E concerns; however, the GTT's capability to support realistic operational testing is dependent upon future Navy decisions to procure sufficient quantity of GTTs.
- All three ships of the *Zumwalt* class share significant new designs, including the unique wave-piercing tumblehome hull form, as well as the new Integrated Power System, Total Ship Computing Environment (software, equipment, and infrastructure), Integrated Undersea Warfare System, Peripheral Vertical Launching System, the AGS, and the associated automated magazines. These systems and equipment have not been subjected to shock testing on previous ship classes. Moreover, the significant automation and relatively small crew may limit the sailors' ability to conduct repairs needed to enable recovery from shock-induced damage.
- Additional AN/SPY-3 radar development and testing at the Wallops Island test facility has significantly compressed the schedule for self-defense testing of the *Zumwalt*-class destroyer and the *Gerald R. Ford*-class nuclear aircraft carrier on SDTS. The completion of this live-fire testing, and the subsequent use of the Probability of Raid Annihilation test bed, is essential to be able to evaluate the self-defense and survivability of the *Zumwalt*-class destroyer. The Navy must identify how the required ship self-defense testing will be completed prior to deployment of a *Zumwalt*-class destroyer. This may mean delaying the AN/SPY-3 radar installation on DDG 1002.
- The Navy has requested funding in FY18/19 to execute a reduced scope component shock qualification program, and is going through the process to identify the equipment/systems and shock grade to which these will be qualified.
  - Indications are that the number of components undergoing shock qualification will be a reduced set, which will introduce risk for the shock trial. Additionally, by reducing the number of components undergoing shock qualification, the assessment of the vulnerability and recoverability capability of the ship at design levels for underwater threats will be limited. The Navy had indicated in prior years that the component shock testing would be funded and conducted prior to installation of any equipment on the first ship, which is the normal, common-sense approach. However, the Navy diverted that funding to other uses; so, the component shock testing was not done and cannot now be done in the normal sequence.
  - Despite these limitations, the shock trials currently scheduled for FY20 must be performed at the traditional severity levels for a surface combatant. These trials will now be the sole source of comprehensive data on the survivability of mission-critical ship systems to shock, and are therefore critical to the success in combat of the ship and her crew.
- The Program Office and the Navy Technical Community encountered problems when attempting to upgrade the survivability M&S tools, which led them to an off-ramp decision to perform the DDG 1000 vulnerability analysis using the existing M&S tools and methods with known shortfalls. The Navy could benefit largely from existing improvements in specific M&S modules by troubleshooting the upgraded M&S modules in a stand-alone mode before integrating them into the over-arching survivability M&S tool that has demonstrated module interface and integration issues. The Navy should also develop a long-term investment strategy to improve the confidence and fidelity levels of its vulnerability and recoverability M&S tools.
- If the *Zumwalt*-class destroyers are not outfitted with LRLAP because of the high cost of the projectiles, the ships will have no capability to conduct Joint Surface Fire Support missions until replacement projectiles are acquired and the AGS is modified to fire the new projectiles. Thus, *Zumwalt*-class destroyers' land attack capability will be limited to TLAMs.
- The currently approved version of the TEMP does not address significant changes to the *Zumwalt*-class destroyer baseline, test strategies and delays in the production schedule. The TEMP revision in Navy routing is required to support operational test.

Recommendations
- Status of Previous Recommendations. The Navy should address the following open recommendations from FY15 and earlier:
  1. Fund and schedule component shock qualification to support the *Zumwalt*-class destroyers' requirement to maintain all mission essential functions when exposed to underwater explosion shock loading.
  2. Develop and conduct an accreditation plan to assess the acceptability of the Probability of Raid Annihilation test bed to support operational testing of the ship's air defense effectiveness.
- FY16 Recommendations. The Navy should:
  1. Complete the revision to the TEMP that accounts for *Zumwalt*-class destroyer baseline changes and system delivery schedule.
  2. Acquire a sufficient quantity of GTTs, when developed, to support testing and fully characterize *Zumwalt*-class destroyer capability to defeat threat torpedoes during FOT&E.
  3. Develop and implement a strategy to address the current limitations with damage predictions in the underwater and air explosion vulnerability assessment tools.
  4. Update DOT&E on the details of the component shock qualification program.
  5. Develop and implement a strategy to complete self-defense testing of the *Zumwalt*-class destroyer on the SDTS.

DDG 51 Flight III Destroyer/Air and Missile Defense Radar (AMDR)/Aegis Combat System

Executive Summary

- On February 10, 2016, the Deputy Secretary of Defense (DEPSECDEF) directed the Navy to adjust funds within existing resources to procure long-lead items to begin procurement of an Aegis/Air and Missile Defense Radar (AMDR)-equipped Self-Defense Test Ship (SDTS). He further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, Evolved SeaSparrow Missile (ESSM) Block 2 programs, document that strategy into draft Test and Evaluation Master Plans (TEMPs), and provide them to DOT&E by July 29, 2016. The Navy has complied with the funding direction but has not complied with the DEPSECDEF direction to provide an integrated test strategy for those programs.
- Despite budgeting for the long-lead AMDR components, the Navy did not program funding in the Future Years Defense Plan to complete all other activities (including procuring Aegis Combat System equipment and targets) necessary to modify the SDTS and support adequate operational testing of the DDG 51 Flight III's self-defense capabilities in FY23 as planned. On November 21, 2016, the DEPSECDEF directed the Navy to fully fund those activities.

System

- The DDG 51 Flight III Destroyer will be a combatant ship equipped with the:
  - AMDR three-dimensional (range, altitude, and azimuth) multi-function radar
  - Aegis Combat System used for air warfare missions and self-defense against anti-ship cruise missiles (ASCMs)
  - AN/SQQ-89 undersea warfare suite that includes the AN/SQS-53 sonar
  - MH-60R helicopter that supports undersea warfare
  - Close-In Weapon System for ship self-defense
  - Five-inch diameter gun for surface warfare and land attack
  - Vertical Launch System that can launch Tomahawk; Standard Missiles 2, 3, and 6; and ESSM Blocks 1 and 2
- The Navy is developing the AMDR to provide simultaneous sensor support of integrated air and missile defense (IAMD) and air defense (including self-defense) missions. IAMD and air defense missions require extended detection ranges and increased radar sensitivity against advanced threats with high speeds and long interceptor fly-out times. The three major components of AMDR are:
  - The AMDR S-band radar that will provide IAMD, search, track, cueing, missile discrimination, air defense non-cooperative target recognition, S-band missile communications, surveillance capability for ship self defense and area air defense, and S-band kill assessment support functions.
  - The AMDR X-band radar – intended to provide horizon and surface search capabilities as well as navigation and periscope detection/discrimination functions – is being delayed. In the interim, the legacy AN/SPQ-9B radar will provide these functions.
  - The AMDR Radar Suite Controller that will provide radar resource management and coordination and an open interface with the ship's combat system.
- The Aegis Combat System is an integrated naval weapons system that uses computers and radars to form an advanced command and decision capability and a weapons control system to track and guide weapons to destroy enemy targets.
- The ESSM, cooperatively developed among 13 nations, is a medium-range, ship-launched, self-defense guided missile designed to defeat ASCM, surface, and low-velocity air threats. There are two variants of ESSM:
  - ESSM Block 1 is a semi-active radar-guided missile that is currently in-service.
  - ESSM Block 2 is in development and will have semi-active radar guidance as well as active radar guidance.
- In comparison to the previous DDG 51 version (Flight IIA), Flight III includes, in addition to the upgraded Aegis Combat System and the AMDR, the following modifications:
  - An upgraded fire extinguishing system
  - New ship service turbine generators
  - Additional transformers
  - Power Conversion Modules

  - Modified controllers for the Machinery Control System and Multifunction Monitors
  - Upgraded air-conditioning plants
- Flight III is also structurally different from the prior DDG 51 version. The design will add starboard enclosures and a stack of small boats, as well as additional structure in the fantail to increase reserve buoyancy and help compensate for additional weight increase. It will also include structural modifications to increase plate thicknesses to lower the ship's center of gravity and enhance girder strength.
- In addition to the self-defense features discussed above, the ship has the following survivability features:
  - Improved ballistic protection for magazines and other vital spaces as well as the inclusion of some shock hardened systems/components intended to enhance survivability.
  - Various installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from peacetime shipboard fire and flooding casualties and from battle damage incurred during combat.

Mission

- Naval Commanders will use the DDG 51 Flight III destroyer equipped with the Aegis Combat System and AMDR to provide joint battlespace threat awareness and defense capability to counter current and future threats in support of:
  - Area air defense (to include self-defense with the ESSM) to counter advanced air and cruise missile threats and increase ship survivability
  - Detecting, tracking, discriminating, and providing missile engagement support (including kill assessment) to counter ballistic missile threats
  - Countering surface threats through surface surveillance, precision tracking, and missile and gun engagements
  - Conducting undersea warfare with periscope detection and discrimination
  - Detecting and tracking own-ship gun projectiles to support surface warfare and naval surface fire support

Major Contractors

- DDG 51 Flight III Destroyer: To be determined. Current DDG 51 destroyer major contractors are:
  - General Dynamics Marine Systems Bath Iron Works – Bath, Maine
  - Huntington Ingalls Industries, Ingalls Shipbuilding Division – Pascagoula, Mississippi
- AMDR: Raytheon – Sudbury, Massachusetts
- Aegis Combat System: Lockheed Martin Marine Systems and Sensors – Moorestown, New Jersey
- ESSM Blocks 1 and 2: Raytheon – Tucson, Arizona

Activity

- On February 10, 2016, the DEPSECDEF directed the Navy to adjust funds within existing resources to procure long-lead items to begin procurement of an Aegis/AMDR-equipped SDTS. He further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, ESSM Block 2 programs and document that strategy into draft TEMPs for those programs to DOT&E by July 29, 2016. The Navy has programmed for long-lead procurement of an AMDR radar face but has not complied with the DEPSECDEF direction to provide an integrated test strategy for those programs despite being provided the integrated operational test plan by DOT&E.
- Despite budgeting for the long-lead AMDR components, the Navy did not program funding in the Future Years Defense Plan to complete all other activities (including procuring Aegis Combat System equipment and targets) necessary to modify the SDTS and support adequate operational testing of the DDG 51 Flight III's self-defense capabilities in FY23 as planned. On November 21, 2016, the DEPSECDEF directed the Navy to fully fund those activities.

Assessment

- DOT&E's assessment is that, absent an AMDR and Aegis-equipped SDTS, the Navy's operational test programs for the AMDR, Aegis Combat System, ESSM Block 2, and DDG 51 Flight III destroyer programs cannot be adequate to fully assess their capabilities, in particular those associated with self-defense. They would also not be adequate to test the following Navy-approved DDG 51 Flight III, AMDR, Aegis Combat System, and ESSM Block 2 requirements.
  - The AMDR Capability Development Document (CDD) describes AMDR's IAMD mission, which requires AMDR to support simultaneous defense against multiple ballistic missile threats and multiple advanced anti-ship cruise missile (ASCM) threats. The CDD also includes an AMDR minimum track range Key Performance Parameter.
  - The DDG 51 Flight III destroyer has a survivability Key Performance Parameter requirement directly tied to meeting a self-defense requirement threshold against ASCMs described in the Navy's Surface Ship Theater Air and Missile Defense Assessment document of July 2008. It clearly states that area defense will not defeat all the threats, thereby demonstrating that area air defense will not completely attrite all ASCM raids and individual ships must be capable of defeating ASCM leakers in the self defense zone.
  - The ESSM Block 2 CDD has a requirement to provide self-defense against incoming ASCM threats in clear and jamming environments. The CDD also includes an ESSM Block 2 minimum intercept range Key Performance Parameter.

- Use of manned ships for operational testing with threat-representative ASCM surrogates in the close-in, self-defense battlespace is not possible due to Navy safety restrictions because targets and debris from intercepts pose an unacceptable risk to personnel at ranges where some of the engagements will take place. The November 2013 mishap on USS *Chancellorsville* (CG 62) involving an ASCM surrogate target resulted in even more stringent safety constraints.
  - In addition to stand-off ranges, safety restrictions require that ASCM targets not be flown directly at a manned ship, but at some cross range offset, which unacceptably degrades the operational realism of the test.
  - Similar range safety restrictions will preclude manned ship testing of five of the seven self-defense ASCM scenarios included in the Navy-approved requirements document for the Aegis Modernization Advanced Capability Build 20 Combat System upgrade and will severely limit the operational realism of the two scenarios that can be flown against a manned ship. Restrictions also preclude testing of the AMDR minimum track range requirement against threat representative ASCM threat surrogates at the land-based AMDR Pacific Missile Range Facility test site.
  - To overcome these safety restrictions for the LHA 6, Littoral Combat Ship, DDG 1000, LPD 17, LSD 41/49, and CVN 78 ship classes, the Navy developed an Air Warfare/Ship Self-Defense Enterprise Modeling and Simulation (M&S) test bed, which uses live testing in the close-in battlespace with targets flying realistic threat profiles and manned ship testing for other battlespace regions, as well as soft-kill capabilities to validate and accredit the M&S test bed. The same needs to be done for the DDG 51 Flight III destroyer with its AMDR, as side-by-side comparison between credible live fire test results and M&S test results form the basis for the M&S accreditation. Without an SDTS with AMDR and an Aegis Combat System, there will not be a way to gather all of the operationally realistic live fire test data needed for comparison to accredit the M&S test bed.
- Since Aegis employs ESSMs in the close-in, self-defense battlespace, understanding ESSM's performance is critical to understanding the self-defense capabilities of the DDG 51 Flight III destroyer.
  - Past DOT&E annual reports have stated that the ESSM Block 1 operational effectiveness has not been determined. The Navy has not taken action to adequately test the ESSM's operational effectiveness.
  - The IOT&E for ESSM Block 2 will be conducted in conjunction with the DDG 51 Flight III destroyer, AMDR, and Aegis Combat System operational testing.
  - Specifically, because safety limitations preclude ESSM firing in the close-in self-defense battlespace, there are very little test data available concerning ESSM's performance, as installed on Aegis ships, against supersonic ASCM surrogates.
  - Any data available regarding ESSM's performance against supersonic ASCM surrogates are from a Ship Self-Defense System-based combat system configuration, using a completely different guidance mode or one that is supported by a different radar suite.
- The cost of building and operating an Aegis SDTS, estimated to be about $350 Million, is small when compared to the total cost of the AMDR development/procurement and the eventual cost of the 22 or more DDG 51 Flight III ships that are planned for acquisition ($55 Billion or higher). Even smaller is the cost of the SDTS compared to the cost of the ships that the DDG 51 Flight III destroyer is expected to protect (approximately $450 Billion in new ship construction over the next 30 years). If DDG 51 Flight III destroyers are unable to defend themselves, these other ships are placed at substantial risk. Therefore, it is essential that the Navy program fully now to support all the tests, targets, and Aegis combat system equipment needed to conduct realistic self-defense testing using an AMDR and Aegis-equipped SDTS.
- The modification/upgrades being planned for DDG 51 Flight III are significant enough to warrant an assessment of the impact of these changes on ship survivability. The Navy has unofficially indicated the DDG 51 Flight III LFT&E strategy will include Component Shock Qualification, a Total Ship Survivability Trial, and a Full Ship Shock Trial. Other LFT&E program particulars are still under discussion to ensure DDG 51 Flight III adequately addresses survivability requirements against operationally relevant threats and recoverability requirements.

Recommendations

- Status of Previous Recommendations. The Navy has not addressed the following previous recommendations. The Navy should:
  1. Program and fully fund an SDTS equipped with the AMDR, ESSM Block 2, and DDG 51 Flight III Aegis Combat System in time to support the DDG 51 Flight III destroyer and ESSM Block 2 IOT&Es.
  2. Modify the AMDR, ESSM Block 2, and DDG 51 Flight III TEMPs to include a phase of IOT&E using an SDTS equipped with the AMDR and DDG 51 Flight III Combat System.
  3. Modify the AMDR, ESSM Block 2, and DDG 51 Flight III TEMPs to include a credible M&S effort that will enable a full assessment of the AMDR, ESSM Block 2, and DDG 51 Flight III Combat System's self-defense capabilities.
  4. Comply with the DEPSECDEF direction to develop and fund a plan, to be approved by DOT&E, to conduct at-sea testing of the self-defense of the DDG 51 Flight III destroyer with the AMDR, ESSM Block 2, and Aegis Combat System.
  5. Provide DOT&E the DDG 51 Flight III LFT&E Strategy for approval in coordination with the TTEMP.
- FY16 Recommendations. The Navy should:
  1. Comply with the DEPSECDEF direction to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, ESSM

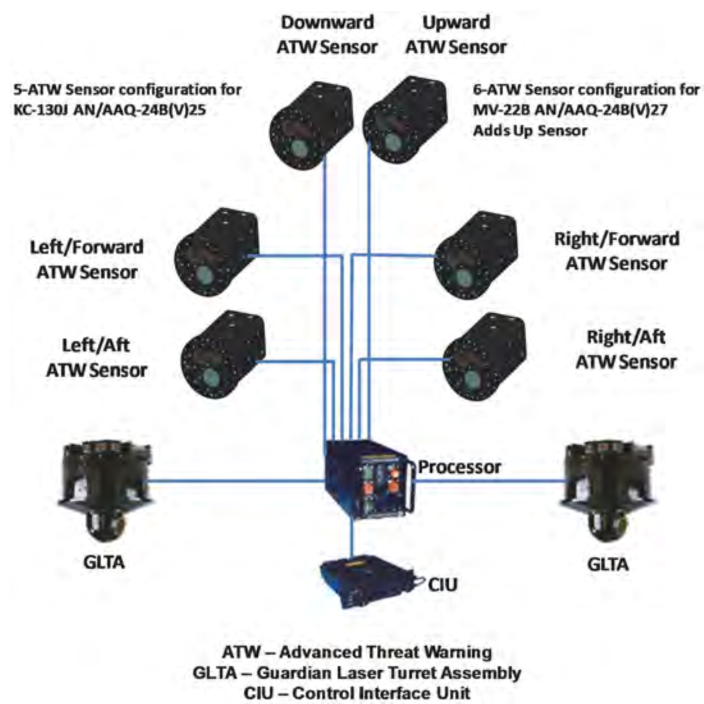
Block 2 programs, and document that strategy into draft TEMPs for those programs to be provided to DOT&E.

2. Program funds in the Future Years Defense Plan to complete all activities and procurements required to conduct adequate operational testing of the DDG 51 Flight III, AMDR, and ESSM Block 2's self-defense capabilities on an Aegis-equipped SDTS scheduled for FY23.
3. Include within the LFT&E Strategy, testing aimed at addressing LFT&E knowledge gaps that can be included in codes/tools designed to assist in determining the platforms' vulnerability and recoverability.

Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM)

Executive Summary

- The Navy conducted developmental tests and continued operational test planning on the Department of the Navy Large Aircraft Infrared Countermeasure (DON LAIRCM) system with the Advanced Threat Warning (ATW) upgrade. The Navy plans for two FOT&E periods in FY17 – one for the MV-22 and one for the KC-130J – as well as a Quick Reaction Assessment for the MV-22.
- The Army conducted integrated developmental/operational testing for installation of the DON LAIRCM ATW system on the Army AH-64, in response to a U.S. Special Operations Command (USSOCOM) Joint Urgent Operational Need (JUON) statement.



System

- The DON LAIRCM system, a variant of the Air Force LAIRCM system, is a defensive system for aircraft designed to defend against surface-to-air infrared missile threats.
- The system combines two-color infrared missile warning sensors with the Guardian Laser Transmitter Assembly (GLTA). The missile warning sensor detects an oncoming missile threat and sends the information to the processor, which then notifies the crew through the control interface unit and simultaneously directs the GLTA to slew to and begin jamming the threat.
- The ATW capability upgrades the processor and missile warning sensors to provide improved missile detection, and adds hostile fire and laser warning capability with visual/audio alerts to the pilots.
- The Navy plans to fully integrate the DON LAIRCM ATW system on the MV-22 and KC-130J with the mission system software.
- The Army plans to integrate AH-64, UH/HH-60, and CH-47 rotary-wing aircraft with the DON LAIRCM ATW system as a federated installation.

Mission

- Commanders employ Marine Corps fixed- and rotary-wing aircraft equipped with DON LAIRCM ATW to conduct medium-lift assault support and aerial refueling of multi-mission aircraft conducting Marine Air-Ground Task Force air operations.
- Commanders employ Army rotorcraft equipped with DON LAIRCM ATW to conduct medium and heavy lift logistical support, medical evacuation, search-and-rescue, armed escort, and attack operations.
- DON LAIRCM ATW will be used during Marine Corps and Army missions to:
  - Provide automatic protection for fixed-wing, tiltrotor, and rotary-wing aircraft against shoulder fired, vehicle-launched, and other infrared-guided missiles
  - Provide automatic hostile fire and laser warning capability for illuminators, beam riders, laser range finders, small arms, rocket-propelled grenades, unguided rockets, and anti-aircraft artillery

Major Contractor

Northrop Grumman, Electronic Systems, Defensive Systems Division – Rolling Meadows, Illinois

Activity

- DOT&E submitted a classified FOT&E report on the DON LAIRCM ATW upgraded installation on the CH-53E in June 2016.
- The Navy conducted developmental tests and operational test planning of DON LAIRCM with the ATW upgrade on the MV-22 and KC-130J between October 2015 and

September 2016. An FOT&E period for the KC-130J and a Quick Reaction Assessment for the MV-22 are planned in FY17.

- The Navy provided materiel support to the Army for the developmental tests and operational test planning for installation of DON LAIRCM with the ATW upgrade on Army AH-64, UH/HH-60, and CH-47 rotary-wing aircraft in response to a USSOCOM JUON.
- The Army began testing the AH-64 installation of DON LAIRCM in 4QFY16 to support the USSOCOM JUON early fielding. Testing was completed in 1QFY17.
- The Navy delayed fielding of the DON LAIRCM ATW upgrade on CH-53E to ensure sufficient quantities of equipment were available to support testing related to the USSOCOM JUON.

Assessment

- DOT&E assessed the DON LAIRCM ATW upgraded installation on the CH-53E as operationally effective but not operationally suitable because of inadequate reliability of the ATW sensors and logistics supportability concerns. The test was adequate to determine both operational effectiveness and operational suitability.
- The Navy is proceeding appropriately during developmental testing on the MV-22 and KC-130J.
  - Developmental test designs were based on lessons learned during previous operational testing.
  - Program delay decisions have been based on results of testing, which have uncovered new failure modes.
  - New failure modes have been identified because of unique mission-based test designs not relevant during previous infrared countermeasure tests on other aircraft.

Recommendations

- Status of Previous Recommendations. The Navy continues to address the previous FY15 recommendations which include:
  1. Continue to improve reliability of the ATW sensors, and monitor and report reliability growth to DOT&E.
  2. Resolve the logistic supportability obsolescence problems with the smart cards used to operate, maintain, and reprogram the DON LAIRCM system.
  3. Resolve the logistic supportability and human factors problem with the location of the control indicator unit.
  4. Resolve the logistic supportability shortfall in the technical documentation and training regarding operational employment aspects of in-flight power cycles.
  5. Collect effectiveness data in a denied-GPS or GPS-jammed environment during FOT&E on either the MV-22 or KC-130J installations of DON LAIRCM.
- FY16 Recommendation.
  1. The Navy should address additional recommendations detailed in the classified June 2016 DOT&E report on the DON LAIRCM ATW installed on the CH-53E.

Distributed Common Ground System – Navy (DCGS-N)

Executive Summary

- The Commander, Operational Test and Evaluation Force (COTF) conducted an FOT&E of the Distributed Common Ground System – Navy (DCGS-N) Increment 1, Block 2 from August 2015 through January 2016.
- On May 9, 2016, DOT&E reported DCGS-N Increment 1, Block 2 to be operationally effective and suitable, but not survivable against cyber threats to the system.
- The USD(AT&L) approved the DCGS-N Increment 2 Milestone B on September 19, 2016.

System

- DCGS-N is the Navy Service component of the DOD DCGS family of systems, providing multi-Service integration of intelligence, surveillance, reconnaissance, and targeting capabilities.
- DCGS-N Increment 1 uses commercial off-the-shelf (COTS) and mature government off-the-shelf (GOTS) software, tools, and standards. It interoperates with the DCGS family of systems via implementation of the DCGS Integration Backbone and Net-Centric Enterprise Services standards.
- Increment 1 is divided into two blocks: Block 1 delivered initial capability on the legacy ship networks, and Block 2 is a hosted application on the Consolidated Afloat Networks and Enterprise Services (CANES).
- Increment 2 will continue to integrate mature COTS and GOTS services and hardware, but it will be hosted on a cloud computing platform provided by CANES for afloat nodes and maritime operations centers (MOCs).
- Increment 2 will be delivered via five Fleet Capability Releases, vice block releases, using an agile development framework. The key additional capabilities for Increment 2 are: enhanced all-source fusion and analysis to provide better maritime domain awareness; enhanced tasking, collection, processing, exploitation, and dissemination; and enhanced sharing of information across commands, Services, and agencies.

Mission

- The operational commanders use DCGS-N to participate in the Joint Task Force-level targeting and planning processes and to share and provide Navy-organic intelligence, reconnaissance, surveillance, and targeting data to Joint Forces.
- Units equipped with DCGS-N will:
  - Identify, locate, and confirm targets through multi-source intelligence feeds
  - Update enemy track locations and provide situational awareness to the Joint Force Maritime Component Commander by processing data drawn from available sensors

Major Contractor

BAE Systems, Electronics, Intelligence and Support (EI&S) – San Diego, California, and Charleston, South Carolina (for Increment 1 only, Increment 2 contractor is TBD)

Activity

- COTF conducted an FOT&E of DCGS-N Increment 1, Block 2 August 2015 through January 2016 onboard the USS *John C. Stennis*. COTF collected performance data during August through November 2015 and declared the end of test on January 11, 2016, after completing cybersecurity testing. Testing was conducted in accordance with the DOT&E-approved test plan.
- DOT&E submitted a classified memorandum report to the Milestone Decision Authority on the results of the Block 2 test on May 9, 2016.
- The USD(AT&L) approved the DCGS-N Increment 2 Milestone B on September 19, 2016.

Assessment

- DOT&E evaluated the Block 2 system to be operationally effective and suitable, but not survivable against cyber threats to the system.
- Additional details can be found in DOT&E's May 2016 classified report.

Recommendations

- Status of FY15 Recommendations. The Navy addressed all previous recommendations.
- FY16 Recommendation.
  1. The Navy should remedy cyber vulnerabilities associated with DCGS-N per DOT&E's classified May 2016 report.

E-2D Advanced Hawkeye

Executive Summary

- In 3QFY16 DOT&E completed its assessment of the E-2D Advanced Hawkeye's first FOT&E period, OT-D1. The focus of OT-D1 was to evaluate the Initial Operational Capability hardware/software configuration, Delta System/Software Configuration (DSSC) Build 1. DOT&E concluded that OT-D1 showed the E-2D had no significant performance difference compared to IOT&E. OT-D1 was adequate to assess E-2D suitability and effectiveness for legacy E-2C missions. Unlike in IOT&E, OT-D1 also executed adequate E-2D carrier testing. An evaluation of E-2D's capability to perform the Theater Air and Mission Defense (TAMD) mission cannot be conducted until future FOT&E periods as that capability is still immature.
- DOT&E approved Change 1 to the E-2D Test and Evaluation Master Plan (TEMP) revision D. The change supports the second FOT&E period (OT-D2), DSSC Build 2, and addresses operational performance relevant to the E-2D system of systems, and E-2D cybersecurity testing,
- The Navy conducted E-2D developmental testing for DSSC-2 between 2QFY16 and 3QFY16. The developmental testing demonstrated DSSC-2 meets required technical performance parameters.

System

- The E-2D Advanced Hawkeye is a carrier-based airborne early warning and command and control aircraft.
- Significant changes to this variant of the E-2 include: upgraded engines, to provide increased electrical power and cooling relative to current E-2C aircraft; a strengthened fuselage, to support increased aircraft weight; replacement of the radar system, communications suite, and mission computer; and incorporation of an all-glass cockpit, which permits the co-pilot to act as a tactical fourth operator in support of the system operators in the rear of the aircraft.
- The radar upgrade replaces the E-2C mechanically scanned radar with a phased-array radar that has combined mechanical and electronic scan capabilities.
- The upgraded radar provides significant improvement in littoral and overland detection performance and TAMD capabilities.
- The E-2D Advanced Hawkeye Program includes all simulators, interactive computer media, and documentation to conduct maintenance, as well as aircrew shore-based initial and follow-on training.
- DSSC-1 included E-2D upgrades and updates to multiple systems such as the radar system, mission computer display, and communication systems. DSSC-2 includes further E-2D upgrades such as improvement in satellite communications, radar, and tracking systems. Future DSSC Builds will focus on the E-2D's Naval Integrated Fire Control – Counter Air (NIFC-CA) capabilities.

Mission

The Combatant Commander, whether operating from the aircraft carrier or from land, will use the E-2D Advanced Hawkeye to accomplish the following missions:

- Theater air and missile sensing and early warning
- Battlefield management, command, and control
- Acquisition, tracking, and targeting of surface warfare contacts
- Surveillance of littoral area objectives and targets
- Tracking of strike warfare assets

Major Contractor

Northrop Grumman Aerospace Systems – Melbourne, Florida

Activity

- The Navy conducted developmental testing for DSSC-2 from 2QFY16 to 3QFY16.
- Change 1 to the E-2D TEMP revision D supports the second FOT&E period (OT-D2), which is scheduled for 4QFY16. Change 1 to revision D E-2D focuses on DSSC-2 upgrades and also includes cybersecurity testing. DOT&E approved the Change 1 TEMP in August 2016.
- DOT&E provided cybersecurity guidance for the OT-D2 cybersecurity test plan and all subsequent test plans and TEMPs for future FOT&E periods.

- The Navy submitted the OT-D2 test plan and a separate cybersecurity test plan, which were both approved by DOT&E in 4QFY16. OT-D2 was completed in 1QFY17 and the operational test report is forthcoming.
- The Navy continues to correct deficiencies with E-2D Cooperative Engagement Capability performance with a plan to have deficiencies remedied in FY19 with fielding of DSSC Build 3.

Assessment

- Following developmental testing for DSSC-2, the Navy concluded that DSSC-2 met the naval requirements for NIFC-CA capabilities. The Navy's Program Executive Officer – Tactical Aircraft Programs subsequently removed NIFC-CA Increment 1 from DSSC-2 for operational testing. The Navy plans to include the NIFC-CA From the Air capability in Increment 2 and include this capability with release to the fleet with DSSC-3 in FY19. Developmental testing demonstrated that the Increment 1 capability lacked sufficient military utility against modern threats. To date, NIFC-CA testing scope has been extremely limited. This limited scope has resulted in a lack of statistical confidence to assess this potential future capability.
- DOT&E's OT-D1 report in 3QFY16 showed that E-2D has no significant performance difference compared to IOT&E and has similar shortfalls on most radar reliability, availability, and weapon system metrics. OT-D1 was adequate to assess E-2D suitability and effectiveness for legacy E-2C missions. An evaluation on E-2D's capability to perform the TAMD mission cannot be made until future FOT&E periods as that capability is immature.
- E-2D's second FOT&E, OT-D2, was completed in 1QFY17. OT-D2 included a separate cybersecurity test plan which was also completed in 1QFY17. An operational test report is forthcoming.
- A full assessment of E-2D operational capabilities will require systematic updates and future operational testing.

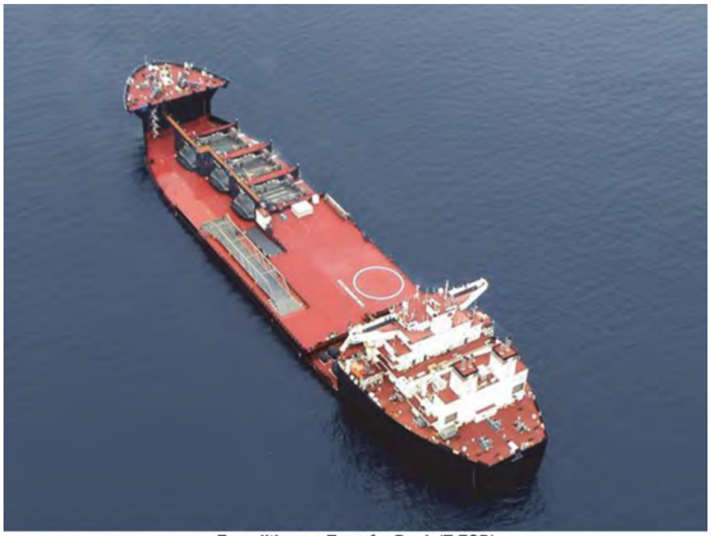
Recommendations

- Status of Previous Recommendations. The Navy continues efforts to improve radar and mission system performance, improve radar and overall weapon system reliability and availability as recommended in FY15. However, these recommendations have not been resolved and thus the Navy should continue to address them.
- FY16 Recommendations. The Navy should:
  1. Incorporate all DOT&E guidance in its cybersecurity testing for OT-D2 and all subsequent FOT&E periods.
  2. Provide complete training on all components of the E-2D system and mission.
  3. As future DSSC updates occur, conduct FOT&E.

Expeditionary Transfer Dock (T-ESD) and Expeditionary Sea Base (T-ESB)

Executive Summary

- From June 2015 through August 2016, the Navy conducted the Expeditionary Sea Base's (T-ESB) Post-Delivery Test and Trials (PDT&T). DOT&E and the Navy's Commander, Operational Test and Evaluation Force (COTF) observed PDT&T events and collected data to be used in the T-ESB's operational assessment.
- In August 2016, the Navy conducted the T-ESB IOT&E, followed immediately by the Total Ship Survivability Trial (TSST).
- DOT&E will publish a combined IOT&E and LFT&E report assessing T-ESB in 2QFY17. The following preliminary assessment is based on observations during IOT&E and PDT&T. The T-ESB:
  - Is capable of hosting a helicopter squadron with four MH-53Es
  - Is capable of hosting all airborne mine countermeasure (AMCM) equipment, including the 7-meter rigid hull inflatable boats (RHIBs) required in the launch and recovery of all waterborne AMCM equipment
  - Is capable of launching, recovering, and maintaining MH-53E helicopters
  - Is capable of deploying all legacy AMCM equipment
  - Is capable of transiting the required 9,500 nautical miles at 15 knots while fully loaded with an AMCM helicopter squadron including all mine-sweeping equipment
  - Lacks enough space to concurrently accommodate personnel and embarked systems of an explosive ordnance disposal detachment and the MCM coordination staff while hosting an AMCM helicopter squadron (not included in the Joint Chiefs of Staff's requirement document)
  - Lacks Chemical, Biological, and Radiological (CBR) defense (not included in the Joint Chief of Staff's requirement document)
  - Has limited self-defense capability against any threat. Its self-defense capability against small boat attacks consists of 12 50-caliber gun stations capable of 360-degree coverage
- The T-ESB was designed to operate in a benign environment where there is low/negligible threat to the ship. However, MCM operations will require the ship to move closer to the MCM threat area. The lack of self-defense capability renders the ship totally dependent upon protection from other naval combatants and joint forces to be survivable in the intended operating environment.
- The Navy conducted the TSST aboard USNS *Lewis B. Puller* (T-ESB 3) August 8 – 9, 2016, in the Virginia Capes operating area. DOT&E's preliminary findings are related to limitations with the internal communication system, emergency lighting, ship egress, and watertight and non-watertight doors. DOT&E will finalize and publish the findings and recommendations in the combined IOT&E and LFT&E report.



Expeditionary Transfer Dock (T-ESD)

Expeditionary Sea Base (T-ESB)

System

- Expeditionary Transfer Dock (T-ESD) and T-ESB are both modified heavy-lift ships, based on the British Petroleum *Alaska*-class oil tanker that the Navy procured to use as logistics interfaces and mobile landing fields, respectively.
- The Navy developed the T-ESD to have the ability to operate from international waters in non-hostile areas, and persist for extended periods of time on station – providing a prepositioning force capability. The T-ESB was developed to provide AMCM support capability both unencumbered by geopolitical constraints to meet strategic goals.
- Military Sealift Command (MSC) serves as the ships' Life Cycle Manager.
- The Navy delivered two T-ESD ships (hulls 1 and 2), one T-ESB ship (hull 3, June 2015), and plans to deliver two more

T-ESB ships. Hull 4 will be delivered in February 2018, and hull 5 will be delivered in September 2019.

- The T-ESD:
  - Includes a vehicle-staging area (raised vehicle deck), vehicle transfer ramp, large mooring fenders, an emergency-only commercial helicopter operating spot, and three Landing Craft Air Cushion (LCAC) lanes/operating spots with wash-down and fueling services
  - Is equipped with a crane and work boat for the placing of fenders used for skin-to-skin operations with the Large Medium Speed Roll-on/Roll-off (LMSR) or Expeditionary Fast Transport (T-EPF) (formerly Joint High Speed Vessel)
  - Requires 34 MSC contracted mariners to operate and maintain the vessel
  - Is built to commercial standards
  - Is classified as a non-combatant
- The T-ESB:
  - Is built similar to the T-ESD to commercial standards. It includes a forward section called the forward house and an aft section called the aft house. The forward house includes military aviation facilities such as a hangar facility; workstations for operation planning; a command, control, communications, computers, and intelligence suite; ammunition magazines for ordnance stowage; and berthing for a total of 250 personnel.
  - During non-hostile periods when the ship is designated as a USNS, it carries 100 permanent military crew and 150 personnel from an embarked detachment. During hostile periods when the ship is designated a USS, it carries 101 permanent military crew and 149 personnel from an embarked detachment. The vessel also has a four-spot flight deck, helicopter fueling capability, and a fueling at-sea station. It houses 34 MSC civilian mariners in the aft house of the ship.
  - Has a mission deck below the flight deck with a man-rated crane for launch and recovery of manned boats, and legacy mine-hunting and mine-clearing equipment, which are used with the MH-53E helicopters during AMCM operations.
  - Has an aft knuckle boom crane rated for 10 metric tons in Sea State 3 (0.50 – 1.25 meters significant wave height) to transfer cargo from the pier to mission deck and/or to the flight deck. This crane is rated up to 8 metric tons to transfer ordnance from mission deck to flight deck or flight deck to mission deck.
  - Has fueling at-sea capability for diesel and JP-5 (jet propellant 5) fuel.
  - Has vertical replenishment capability.
  - Is classified as a non-combatant.
- The T-ESD and T-ESB designs inherently incorporate survivability features evaluated through the LFT&E program, to include:
  - Distributed firefighting equipment in the form of a fire main and aqueous film-forming foam and distributed damage control lockers/repair stations (containing fire hoses, firefighting ensembles, self-contained breathing apparatus, and flood repair kits).
  - Retractable bow thruster for station-keeping.
  - Emergency electrical power to selective ship loads by way of the Emergency Diesel Generator (EDG).
  - A carbon dioxide gaseous flooding system in the main engineering, EDG spaces, and spaces with high risk of fuel induced fires.
  - As a result of its more aviation focused mission, the T-ESB is equipped with an Aviation Crash Locker to handle shipboard aviation casualties and a seawater sprinkling system for protection to magazines and other high-risk spaces in the forward portion of the ship.

Mission

- Combatant Commanders will use the T-ESD to support Mobile Prepositioning Force (future) operations by facilitating at-sea transfer and delivery of prepositioned assets to units ashore. The T-ESD will act as a vessel interface between LMSR or T-EPF and LCAC vehicles and, in the future, Ship-to-Shore Connectors.
- Combatant Commanders will use the T-ESB to support AMCM operations, which includes hosting a squadron of four legacy MH-53E helicopters together with their mine-clearing equipment, or explosive ordnance demolition teams with their equipment.
- Special Operations Force (SOF) will use the T-ESB to support Helicopter Assault Force and Boat Assault Force operations, not concurrently with AMCM operations.

Major Contractors

- Base ship for both variants and T-ESB mission package: General Dynamics' National Steel and Shipbuilding Company (NASSCO) – San Diego, California
- T-ESD mission package: Vigor Marine LLC Shipbuilding – Portland, Oregon

Activity

T-ESD

- There were no T-ESD test events in FY16.

T-ESB

- On December 8, 2015, DOT&E approved the T-ESB IOT&E test plan. The test plan adopted an integrated test approach where the Navy conducted developmental and operational testing concurrently, with each having its own set of metrics and data collection. All operational tests were conducted in accordance with the DOT&E-approved test plan.
- The first ship of the class, USNS *Lewis B. Puller* (T-ESB 3), launched in November 2014, completed builder trials in

April 2015, and acceptance trials in May 2015; and was delivered to the Navy in June 2015.

- T-ESB 3 transited from San Diego, California, to Norfolk, Virginia, from August to October 2015. COTF collected material availability data from the ship's crew during the transit.
- Personnel from the Naval Surface Warfare Center, Port Hueneme, California, conducted an Underway Replenishment Ship Qualification Trial in January 2016, off the coast of Norfolk, Virginia.
- Combat Direction Systems Activity personnel observed by COTF completed two phases of cybersecurity developmental testing: the first phase in November/December 2015, and the second phase in January/February 2016.
- Combatant Craft Division of Naval Surface Warfare Center Carderock Division completed two phases of craft launch and recovery testing, first in February 2016, and then again in May 2016.
- The Board of Inspection and Survey conducted a Final Contract Trial in April 2016.
- Naval Air Systems Command with aircraft and maintenance detachment provided by Helicopter Mine Countermeasure Squadron-15 (HM-15), conducted Aircraft Dynamic Interface Testing, including Vertical Replenishment operations, during April and June 2016.
- The Program Office, assisted by HM-15, conducted AMCM deployment test during PDT&T in June 2016.
- The Program Office, assisted by MSC's Afloat Training Team, completed the TSST aboard USNS *Lewis B. Puller* (T-ESB 3) August 8 – 9, 2016, off the coast of Norfolk, Virginia, in the Virginia Capes operating area. This event was preceded by pre-test system checks to verify system components and line-ups in November 2015 and January and May 2016.
- COTF personnel:
  - Observed a ship self-defense test contending crew-served weapons against high-speed maneuvering surface targets in May 2016 on USS *San Antonio* (LPD 17)
  - Conducted the cybersecurity Cooperative Vulnerability and Penetration Assessment during May and June 2016, and the cybersecurity Adversarial Assessment during July 2016
  - Conducted the IOT&E End-to-End Event in accordance with the DOT&E-approved test plan in August 2016, while underway in the Virginia Capes operating area
  - Conducted a critical systems maintenance review, consisting of targeted interviews with senior military and civilian crewmembers, onboard the ship while in port at Naval Station Norfolk during August 2016
  - Conducted a walk-through SOF review with the subject matter experts to assess the ship's ability to host light-package SOF missions onboard the ship, while in port at Naval Station Norfolk during August 2016
- The 1-year post-delivery guarantee period ended on June 11, 2016.

Assessment

T-ESD

- The results from earlier testing were reported in the July 6, 2015, DOT&E combined IOT&E and LFT&E report on Mobile Landing Platform with Core Capability Set (MLP (CCS)).

T-ESB

- T-ESB's preliminary findings are based on observations on USNS *Lewis B Puller* (T-ESB 3) during the PDT&T and IOT&E periods. DOT&E will provide the final assessment in the 2QFY17 combined IOT&E and LFT&E report.
  - Based on a 24-hour fuel endurance trial, DOT&E estimates T-ESB to have an un-refueled range of greater than 11,000 nautical miles, exceeding the 9,500-nautical mile requirement.
  - Out of the four helicopter operating spots on the flight deck, three are functional for landing and launching MH-53E helicopters while performing the AMCM mission. The fourth spot served as a parking space only, since it was fouled by a triple wide container used for AMCM equipment. Without this container, the fourth spot is fully functional.
  - The helicopter hanger is large enough to accommodate two folded or one spread MH-53E helicopters.
  - The ammunition magazines can accommodate AMCM ordnance such as the SeaFox mine disposal vehicle.
  - The mission deck size and tie down arrangement are sufficient to accommodate all supplies and equipment required for a four-helicopter MH-53E Squadron including all legacy mine-sweeping equipment.
  - The mission deck crane is effective for launching and recovering all AMCM equipment along with launching the 7-meter RHIBs used for deploying the AMCM equipment. The mission deck crane is also effective for launching and recovering the 11-meter RHIBs and 41-foot Combatant Craft Assault boats.
  - Cybersecurity test results and analysis will be provided in the classified annex to the 2QFY17 DOT&E combined IOT&E and LFT&E report.
  - The lack of air conditioning in the aircraft maintenance shops surrounding the hanger bay will limit work days for maintainers in high heat stress areas of the world.
  - Lacks enough space to concurrently accommodate personnel and equipment of an explosive ordnance detachment, the MCM staff required to coordinate the operations, and an AMCM helicopter squadron during the MCM operations. This may affect the MCM mission.
- The T-ESD and T-ESB are built to commercial standards and have survivability features to protect against typical commercial ship hazards such as groundings, collisions, raking, and fires. However, for missions that the ships will execute in the littorals close to threat areas, not having military survivability requirements introduce the following shortfalls:

  - Lack of a CBR defense capability, including countermeasure wash-down capability
  - Lack of anti-ship missile, torpedo, and naval mine defense capability
  - Self-defense capability is limited to crew-served weapons only
- The T-ESB was designed to operate in a benign environment where there is low/negligible threat to the ship. However, MCM operations will require the ship to move closer to the MCM threat area. The lack of self-defense capability renders the ship totally dependent upon protection from other naval combatants and joint forces to be survivable in the intended operating environment.
- T-ESB has very limited self-defense capability, which will force the Combatant Commander to place T-ESB outside the threat area. Alternately, the Combatant Commander will need to devote defensive units to support the mission. T-ESB is not outfitted to accommodate explosive ordnance teams or mine clearing coordination staffs while supporting AMCM.
- The T-ESB TSST identified limitations with the ships' communications systems that challenged the damage control effectiveness of both the Navy and MSC crew. Additionally, the trial revealed ship design deficiencies associated with emergency lighting, personnel egress, and the ships' watertight and interior joiner doors. The Navy is assessing the TSST data and will provide additional findings in their report due in FY17. DOT&E will finalize and publish findings and recommendations in the combined IOT&E and LFT&E report.
- If T-ESB is upgraded to add full SOF capability, an FOT&E event will be required to evaluate the added SOF capability. The final DOT&E IOT&E and LFT&E report will provide assessment based on the walk-through review that COTF conducted with existing SOF capability during the end-to-end test event.

Recommendations

- Status of Previous Recommendations: The Navy still needs to address the FY14 recommendation to re-evaluate the need for at-sea skin-to-skin operations between T-ESD and T-EPF. The Navy also still needs to address the following FY15 recommendations:
  1. Install a separate Ship Service Diesel Generator to minimize periods of under-loading of the Main Diesel Generators.
  2. Address the live fire issues identified in the classified annex to the July 2015 DOT&E combined IOT&E and LFT&E report on the T-ESD.
  3. Conduct a robust, self-defense test utilizing live ammunition and realistic targets in support of the T-ESB IOT&E.
- FY16 Recommendation.
  1. DOT&E will provide recommendations regarding test adequacy, effectiveness, suitability, and survivability of the T-ESB in the combined IOT&E and LFT&E report in FY17 after a more comprehensive analysis of all operational and live fire test data.

F/A-18E/F Super Hornet and EA-18G Growler

Executive Summary

- During FY16, the Navy released System Configuration Set (SCS) H10E for use in the F/A-18E/F Super Hornet and the EA-18G Growler fleets. Software upgrades for the Super Hornet included improved multi-sensor integration, aircrew displays, short-range tracking, and combat identification. For the Growler, SCS H10 added the Joint Tactical Terminal Receiver, enhanced combat identification capability, and expanded jamming assignments. SCS H10 included an initial capability allowing aircrew for both platforms to operate more easily in Air Traffic Control (ATC)-controlled airspace.
- The reliability of the APG-79 Active Electronically Scanned Array (AESA) radar improved during SCS H10 testing for the F/A-18E/F and EA-18G, demonstrating the highest reliability to date since introduction of the AESA in 2006. However, it failed to meet the program reliability requirement.
- SCS H10 built-in test (BIT) detection and isolation functions demonstrated strong performance, but a high BIT false alarm rate resulted in an unnecessary maintenance burden.
- The Super Hornet weapons system has demonstrated operational effectiveness and suitability in most, but not all, threat environments. Previous DOT&E classified reports have discussed the threat environments in which the Super Hornet is not effective.
- The EA-18G Growler weapons system equipped with SCS H10 demonstrated operational effectiveness and suitability with the same radar limitations as the Super Hornet. It also demonstrated degraded APG-79 performance when ALQ-99 pods radiated within the AESA frequency range.
- The Navy began operational testing of the next software upgrade, SCS H12, in October 2016. Planned improvements include another phase of multi-sensor integration improvements, enhanced ALQ-218 geolocation, Communication Countermeasures Set improvements, modifications to crew to aircraft interfaces and displays to manage aircrew workload, and additional capabilities to operate in ATC-controlled airspace.

System

F/A-18E/F Super Hornet

- The Super Hornet is the Navy's premier strike-fighter aircraft and is a more capable follow-on replacement to the F/A-18A/B/C/D and the F-14.
- F/A-18E/F Lot 25+ aircraft provide functionality essential for integrating all Super Hornet Block 2 hardware upgrades, which include:
  - Single pass multiple targeting for GPS-guided weapons
  - Use of off-board target designation
  - Improved datalink for target coordination precision
  - Implementation of air-to-ground target aim points
- Additional systems include:

  - APG-73 (Lots 21-24) or APG-79 radar (Lots 25+)
  - Advanced Targeting Forward Looking Infrared Systems
  - AIM-9 infrared-guided missiles and AIM-120 and AIM-7 radar-guided missiles
  - Multi-functional Information Distribution System for Link 16 tactical datalink connectivity
  - Joint Helmet-Mounted Cueing System
  - Integrated Defensive Electronic Countermeasures

EA-18G Growler

- The Growler is the Navy's land- and carrier-based, radar and communications jamming aircraft.
- The two-seat EA-18G replaces the four-seat EA-6B Prowler. The ALQ-218 receiver, improved connectivity, and linked displays are the primary design features implemented to reduce the operator workload in support of the EA-18G's two-person crew.
- The Airborne Electronic Attack (AEA) system includes:
  - Modified EA-6B Improved Capability III ALQ-218 receiver system
  - Advanced crew station
  - Legacy ALQ-99 jamming pods
  - Communication Countermeasures Set System
  - Expanded digital Link 16 communications network
  - Electronic Attack Unit
  - Interference Cancellation System that supports communications during jamming operations
  - Satellite receiver capability via the Multi-mission Advanced Tactical Terminal
- Additional systems include:
  - APG-79 AESA radar
  - Joint Helmet Mounted Cueing System
  - High-speed Anti-Radiation Missile
  - AIM-120 radar-guided missiles

System Configuration Set (SCS) Software

- Growler and Super Hornet aircraft include SCS operational software to enable major combat capabilities. All EA-18G

and Block 2 F/A-18E/F (production Lot 25+) use high-order language (HOL) "H-series" software, while F/A-18E/F prior to Lot 25 and all legacy F/A-18A/B/C/D aircraft use "X-series" software.
  - The Navy released SCS H10 in October 2015 and began operational testing of SCS H12 in October 2016.
  - The Navy released SCS 25X on legacy Hornet and older Super Hornet aircraft in October 2015.

Mission

- Combatant Commanders use the F/A-18E/F to:
  - Conduct offensive and defensive air combat missions.
  - Attack ground target with most of the U.S. inventory of precision and non-precision weapons.
  - Provide in-flight refueling for other tactical naval aircraft.
  - Provide the fleet with an organic tactical reconnaissance capability.
- Combatant Commanders use the EA-18G to:
  - Support friendly air, ground, and sea operations by countering enemy radar and communications
  - Jam integrated air defense systems
  - Support non-integrated air defense missions and emerging non-lethal target sets
  - Enhance crew situational awareness and mission management
  - Enhance connectivity to national, theater, and tactical strike assets
  - Provide enhanced lethal suppression through accurate High-speed Anti-Radiation Missile targeting
  - Provide the EA-18G crew with air-to-air self-protection with the AIM-120

Major Contractors

- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri
- Raytheon Company – Forest, Mississippi
- General Electric Aviation – Evendale, Ohio
- Northrop Grumman Corporation – Bethpage, New York

Activity

- The Navy released SCS H10 to the F/A-18E/F and EA-18G fleets in 2016.
- The Navy began testing SCS H12 on both platforms in October 2016 in accordance with a DOT&E-approved test plan. Testing will continue into 2017.
- The Navy delivered SCS H10 improvements for the Super Hornet including improved multi-sensor integration, aircrew displays, short-range tracking, combat identification, and the ability to operate more easily in ATC-controlled airspace.
- The Navy delivered SCS H10 improvements for the Growler including the addition of the Joint Tactical Terminal Receiver, enhanced combat identification, expanded jamming assignments, and the ability to operate more easily in ATC-controlled airspace.
- The Navy completed testing and released SCS 25X to the fleet in 2016 for use in F/A-18 A-D and early lot F/A-18E/Fs that do not have HOL computers. The Navy plans to use the remaining non-HOL Super Hornets primarily for training.

Assessment

- Although capability enhancements in SCS H10 resulted in incremental changes in the ability of the Super Hornet to complete missions, DOT&E did not expect this software release to add significant mission capability. The F/A-18E/F remains operationally effective in some threat environments and ineffective in particular air warfare environments noted in classified reports. Though SCS H10 has begun to address some of those long-standing deficiencies in air warfare, the Super Hornet requires further improvements. Software false alarms in SCS H10 impose a maintenance burden on unit personnel.
- SCS H10 testing showed improved AESA reliability, and while it demonstrated the highest reliability to date since introduction of the AESA in 2006, it fell short of its reliability requirement. Although the AESA provides improved performance compared to the legacy mechanically-steered radar, DOT&E has assessed the radar as not operationally suitable since the 2006 IOT&E because of poor software stability and BIT performance. Fault identification and isolation functionality have improved, but the AESA false alarm rate remains high. Additionally, the F/A-18 has demonstrated interoperability deficiencies with on- and off-board sensor inputs.
- DOT&E continues to assess the EA-18G as operationally effective and suitable subject to the same threat limitations as the Super Hornet. The radar performance degradation occurs when ALQ-99 pods radiate in AESA frequencies, affecting Growler operational effectiveness.
- Because the Navy did not include an end-to-end multiple AIM-120 missile test during SCS H10, testing has been deferred to SCS H12 FOT&E. The Navy will not have successfully demonstrated that the AESA can support this required capability until this test is successfully completed.
- The Navy's F/A-18 fleet relies more heavily on Lot 25+ E and F aircraft compared to the Navy's operational test squadron, VX-9, which includes more F/A-18C and D aircraft and older E and F aircraft that lack HOL mission computers and APG-79 AESA radars, making test conditions less operationally representative.

Recommendations

- Status of Previous Recommendations. Per previous recommendations, the Navy should continue to improve the

APG-79 radar reliability, false alarm performance, and, for the EA-18G, geolocation timeliness with jammers off, and should continue to develop and characterize the full electronic warfare capability of the AESA radar. DOT&E continues to recommend that the Navy conduct an operationally representative end-to-end missile test to demonstrate APG-79 radar and system support for a multiple AIM-120 missile engagement. The Navy should continue to focus on improvements that will allow the Super Hornet and Growler to be operationally effective in all threat environments.

- FY16 Recommendation.
  1. The Navy should upgrade the Super Hornet aircraft used during operational testing to better reflect fleet composition in terms of number of aircraft with HOL mission computers and APG-79 radars.

Infrared Search and Track (IRST)

Executive Summary

- On November 5, 2015, the USD(AT&L) designated the Infrared Search and Track (IRST) program as an Acquisition Category (ACAT) I program and delegated milestone decision authority to the Navy.
- The Commander, Operational Test and Evaluation Force (COTF) conducted Operational Assessment 2 (OA 2) in November 2015. OA 2 included simulated air combat against a challenging, operationally realistic threat surrogate. The system continues to have difficulty with detection and tracking in an environment that reflects realistic fighter employment and tactics. DOT&E reported OA 2 results in a January 27, 2016, classified memorandum.
- Assistant Secretary of the Navy (ASN) for Research, Development, and Acquisition (RDA) held an IRST program review on January 27, 2016, and in a September 8, 2016, Acquisition Decision Memorandum (ADM), ASN (RDA) approved a restructured program that foregoes full-rate production of Block I sensors and proceeds directly to development of the Block II system. The Block I system will not be fielded and IOT&E did not begin in 2016 as planned.
- The Navy plans to hold the Block II Preliminary Design Review in May 2017 and begin IOT&E in 2020.

System

- The IRST system consists of a passive long-wave infrared receiver (IRR), a processor, inertial measurement unit (IMU), and environmental control unit (ECU). The IRR, processor, IMU, and ECU are housed within the Sensor Assembly Structure (SAS). The SAS attaches to the front of the Fuel Tank Assembly that is mounted to the aircraft on the BRU-32 bomb rack. The Navy designed the IRST to be flown on the F/A-18E/F and it will be built into a modified centerline fuel tank.
- The Navy developed Block I using components from the F-15K/SG IRR, which is based on the F-14 IRST design. Block I will be used to support testing and tactics development. Block II is being acquired through an Engineering Change Proposal contract as an engineering change to Block I. Block II will include improvements to the IRR and updated processors.
- The Navy intends to produce a total of 170 IRST systems. The 18 Block I low-rate initial production (LRIP) systems will be retrofitted to the Block II configuration and an additional 152 Block II systems will be acquired.

Mission

Commanders will use F/A-18E/F aircraft equipped with the IRST in a radar-denied environment to locate and destroy enemy forces. The IRST system is intended to allow the F/A-18E/F to operate and survive against existing and emerging air threats by enhancing situational awareness and providing the ability to acquire and engage targets beyond visual range.

Major Contractors

- The Boeing Company – St Louis, Missouri
- Lockheed Martin – Orlando, Florida

Activity

- The USD(AT&L) designated IRST as an ACAT IC program on November 5, 2015.
- COTF conducted OA 2 in November 2015. VX-9, with support from VX-31, conducted realistic engagements over the China Lake Range Complex and Point Mugu Sea Range. DOT&E reported results in a January 27, 2016, classified memorandum.
- ASN (RDA) held an IRST program review on January 27, 2016, to consider LRIP-2 and receive a program status update.
- Following the ASN (RDA) review, the Navy developed a new program plan, which foregoes full-rate production of Block I after the acquisition of the 18 LRIP units and proceeds directly to the development of the Block II system, which is expected to enter IOT&E in 2020. Under the new plan, the Block I LRIP units will not be fielded, but will be used for testing and tactics development until they can be retrofitted to the Block II configuration.
- In a September 8, 2016, ADM, ASN (RDA) approved Block I LRIP-2 (12 units) and entry into the Block II development phase.

- Based on the results of aeromechanical testing, Naval Air Systems Command (NAVAIR) issued a flight clearance in July that allowed flight test with the full envelope of flight conditions when the fuel tank is empty and excludes a small set of conditions when the tank has over 500 pounds of fuel (and an even narrower set of conditions with more than 1,500 pounds of fuel). The new flight clearance also clears the fuel tank for shore-based catapults and arrestments (with less than 230 pounds of fuel). Since the July flight clearance was issued, Boeing has released their carrier suitability report, which recommends IRST for unrestricted carrier operations. The Program Office provided the results to NAVAIR engineering, which are reviewing them, and will release an updated flight clearance if appropriate.
- The program has increased the scope of Integrated Test Phase IT-C1 to include testing IRST on aircraft software System Configuration Set (SCS) H14 and will extend the test phase through summer 2017. The objectives of this test phase are to characterize sensor performance (including testing algorithm enhancements intended to improve performance) and test integration of IRST with the F/A-18 weapons system. Testing also includes a progression of simulated AIM-120 shots on IRST tracks using captive carry missiles. The culminating live weapons shots planned for Block I were canceled.

Assessment

- The Key Performance Parameter (KPP) and the derived contract specification for detection and tracking describe only a narrow subset of the operational environments where the Navy will employ IRST. Meeting the KPP (with a narrow reading of the KPP requirement) does not ensure a useful combat capability. Much of developmental testing, however, was focused on verifying this contract specification.
- OA 2 included realistic operational conditions. The system tested in OA 2, while much improved from OA 1, could not reliably detect and track targets well enough to support weapons employment in an environment that reflects realistic fighter employment and tactics.
- Demonstrated reliability is below what was expected at this point in the flight test program. As of the time of DOT&E's OA 2 report, the cumulative Mean Time Between Operational Mission Failure (MTBOMF) was 4.1 hours; the reliability after incorporating known fixes was 19.5 hours. The MTBOMF requirement is 40 hours and the system was expected to have a projected reliability of 38 hours when entering IOT&E.
- Most of the failures are built-in test (BIT) false alarms that require a system reset and are therefore scored as an OMF.
- The Block II system has significant commonality with the Block I system. Block I will continue to fly between now and the start of Block II IOT&E. If the program keeps in place its reliability growth program, identifying and correcting failure modes, the reliability of components that Block II has in common with Block I should improve.
- The Block I system reliability growth plan was overoptimistic in its assessment of initial reliability. A new reliability growth plan is needed for Block II and care should be taken to determine a realistic initial reliability and growth rate. While reliability has grown with Block I and projected reliability at the time of OA 2 was 19.5 hours, new hardware and software might initially reduce Block II reliability. Achieving the desired reliability could require a design effort focused on the reliability of the BIT system in order to meet the 40-hour threshold requirement. The program should also consider reviewing the rationale for the current reliability threshold.
- The logistical impact of requiring a mechanical boresight procedure for Block II should be considered for the Block II sensor design.
- The new flight clearance is a significant improvement over the flight clearance used in OA 2. Given the rate at which fuel is consumed from the centerline fuel tank, these restrictions are effective for only a short period at the beginning of the mission profile and should not have an operational impact.
- Many of the Block I system's difficulties with detection and tracking seen in OA 1 and OA 2 did not require flight testing to uncover them, but could have been discovered earlier via analysis and modeling and simulation. The Navy expects that the Block II configuration (which includes sensor and aircraft hardware and software), will provide improved capability. This assumption should be tested as early as possible, prior to major decisions, via analysis and modeling and simulation if flight test data are not available. The program has a wealth of data and lessons learned that could be used to support such an effort.

Recommendations

- Status of Previous Recommendations. The Navy should continue to address the two FY15 recommendations:
  1. Explicitly state detection and tracking requirements for the range of operational conditions in which the Navy expects to employ the system. The requirements document has not been updated. Testing, however, has included operationally realistic conditions and COTF and DOT&E have evaluated the system against the stated mission need.
  2. Improve detection and tracking performance prior to entry into IOT&E. The Navy has elected not to proceed beyond LRIP with Block I and will wait until the Block II sensor and SCS H16 aircraft software are available prior to entering IOT&E.
- FY16 Recommendations. The Navy should:
  1. Use modeling and simulation and analysis (including analysis of Block I data) to test the detection and tracking capability of the Block II system as early as possible, well prior to flight test. Document this strategy in the updated Test and Evaluation Master Plan.
  2. Future developmental testing should include more testing beyond specification compliance to ensure readiness to conduct operationally representative missions in operational testing and in combat.
  3. Correct issues seen in the Block I in-flight transfer alignment system or include the necessary logistical support for mechanical boresight in the Block II design.

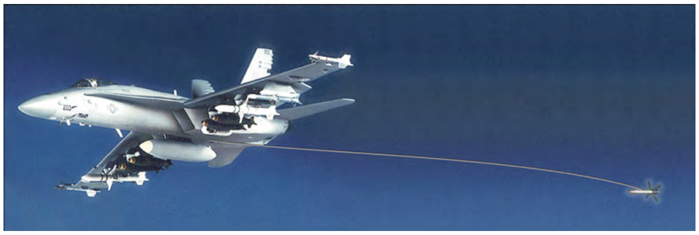
Integrated Defensive Electronic Countermeasures (IDECM)

Executive Summary

- The Navy completed an Integrated Defensive Electronic Countermeasure (IDECM) Software Improvement Program (SWIP) operational assessment (OA) on September 30, 2015. Developmental testing of the SWIP program is ongoing, and integrated test missions flew in July and August 2016, at the Joint Pacific Alaska Range Complex (JPARC) at Eielsen AFB near Fairbanks, Alaska.
- The Navy's F/A-18 wingman radio frequency compatibility group that contains members from multiple Navy Program Offices continues to investigate and resolve deficiencies associated with the aircraft radar, which may be caused by other systems such as IDECM. The Navy has asked for significant funding to resolve the incompatibilities.
- DOT&E produced a classified report on the IDECM SWIP OA and the integrated testing at JPARC. The IDECM Block 4 hardware is effective and suitable on the F/A-18E/F, and not effective and not suitable on the F/A-18C/D because the system is unsafe due to environmental control system issues leading to cabin pressurization problems.
- The IDECM Block 4 with SWIP demonstrated inconsistent performance during integrated testing at the JPARC. However, the system demonstrated improved stability over previous developmental test flights.

System

- The IDECM system is a radio frequency, self-protection electronic countermeasure suite on F/A-18 aircraft. The system is comprised of on- and off-board components. The onboard components receive and process radar signals and can employ on- and/or off-board jamming components in response to identified threats.
- There are four IDECM variants: Block I (IB-1), Block II (IB-2), Block III (IB-3), and Block IV (IB-4). All the variants include an onboard radio frequency receiver and jammer.
  - IB-1 (fielded FY02) combined the legacy onboard receiver/jammer (ALQ-165) with the legacy (ALE-50) off-board towed decoy.
  - IB-2 (fielded FY04) combined an improved onboard receiver/jammer (ALQ-214) with the legacy (ALE-50) off-board towed decoy.
  - IB-3 (fielded FY11) combined the improved onboard receiver/jammer (ALQ-214) with a new (ALE-55) off-board fiber-optic towed decoy that is more integrated with the ALQ-214.
  - IB-4 with SWIP (currently in developmental test) replaces the onboard receiver/jammer (ALQ-214(V)3) with a lightweight, repackaged onboard jammer (ALQ-214(V)4 and ALQ-214(V)5). IB-4 also replaces the ALQ-126B to provide advanced, carrier capable jamming to the F/A-18C/D for the first time. IB-4 (without SWIP) fielded to three squadrons in FY15.



- IB-4 hardware will run enhanced onboard software known as SWIP. SWIP will give IDECM enhanced capabilities against modern threats, denying or delaying a weapons-quality track on the F/A-18.
- The F/A-18E/F installation includes off-board towed decoys. The F/A-18C/D installation includes only the onboard receiver/jammer components and not the towed decoy.

Mission

- Combatant Commanders will use IDECM to improve the survivability of Navy F/A-18 strike aircraft against radio frequency-guided threats while flying air-to-air and air to ground missions.
- The Navy intends to use IB-4's complex jamming capabilities to increase survivability against modern radar guided threats.
- IDECM SWIP provides a new deny/delay capability to enhance survivability against modern radio frequency threats.

Major Contractors

- ALE-55: BAE Systems – Nashua, New Hampshire
- ALQ-214: Harris – Clifton, New Jersey
- ALE-50: Raytheon Electronic Warfare Systems – Goleta, California

Activity

IB-4

- The Navy completed an OA for IDECM Block 4 hardware on September 30, 2015. Testing was adequate to assess effectiveness on the F/A-18E/F. However, due to a major safety issue on the F/A-18C/D, the Navy deferred testing on F/A-18C/D until the middle of FY-17.
  - All planned laboratory testing, including a dense emitter scenario and closed-loop hardware-in-the-loop testing was completed.
  - Follow-on testing is scheduled for 2017 to complete all remaining flight test points for both platforms.

IB-4 with SWIP

- The Navy completed integrated testing at a hardware-in-the-loop facility for the SWIP software.
  - Integrated testing at the JPARC tested the SWIP system against a modern threat in a more realistic threat environment than was previously possible. Further, while working in concert with the EA-18G and the ALQ-99 jamming pod, the Navy tested SWIP interoperability and effectiveness in the presence of support jamming.
  - Due to the integrated nature of the test, multiple configurations and software versions were tested at the JPARC.
- The Navy conducted all testing in accordance with a DOT&E-approved test plan.

Assessment

IB-4

- IDECM Block 4 is effective and suitable on the F/A-18E/F and unsafe and not suitable on the F/A18C/D, leading to a not effective evaluation. Testing was adequate to support DOT&E evaluation of the system.
  - IDECM Block 4 demonstrated the same capabilities as the legacy IDECM Block 3 system.
  - Environmental Control System (ECS) problems on multiple F/A-18C/D aircraft prevented completion of IDECM Block 4 testing. Since the root cause of the ECS issues has not been determined, IDECM Block 4 is unsafe on the F/A-18C/D. The Navy wrote technical orders to diagnose ECS problems on the F/A-18C/D, but each aircraft must be investigated individually to solve the problems. IDECM is therefore not suitable on the F/A-18C/D fleet writ large.

IB-4 with SWIP

- IDECM Block 4 with SWIP demonstrated little deny-delay capability at the JPARC against a modern threat. The IDECM program should optimize countermeasure techniques employed using SWIP and their effectiveness for the threats of interest.
- IDECM Block 4 with SWIP did not demonstrate consistent effectiveness against modern surface-to-air missile systems. Integrated test led to the discovery of stability problems with the SWIP software, some of which have potential fixes in the latest software, but system effectiveness is often unpredictable. On at least one occasion, the SWIP system produced no radio frequency output but all system indications showed that IDECM was working perfectly.

Recommendations

- Status of Previous Recommendations. The Navy addressed some previous recommendations; however, the following remain outstanding:

IDECM System

1. The Navy should develop hardware and/or software changes to provide pilots with correct indications of whether a decoy was completely severed. This recommendation does not apply to the F/A-18 C/D installation since that installation does not include a towed decoy.
2. The Navy should continue to improve maintenance data collection processes and reporting methods during developmental and integrated test for IDECM to support an adequate suitability assessment.
3. The Navy should ensure that the ALR-67(V)3 Radar Warning Receiver interface with IDECM is updated to allow for proper situational awareness when SWIP is in use.
4. The Navy should ensure that the SWIP software is consistent and produces effective output prior to fielding.

Electronic Warfare Warfighting Improvements

5. In coordination with the Defense Intelligence Agency, the Navy should update the warhead probability of kill data in requirements documents to confirm IDECM effects are sufficient to ensure aircraft survivability.
6. The Services should improve the fidelity of missile endgame analysis, to including warhead fuzing.

- FY16 Recommendations. The Navy should:
  1. Fully resolve F/A-18C/D ECS issues before resuming any test flights on the F/A-18C/D.
  2. Determine for each threat whether the current SWIP techniques or the original IDECM Block 3 or 4 baseline techniques provide the greatest survivability gains and field the most effective technique.

Joint Standoff Weapon (JSOW)

Executive Summary

- The Navy completed Joint Standoff Weapon (JSOW) C-1 operational testing and declared Initial Operational Capability (IOC) in FY16.
- DOT&E published a classified FOT&E report in early FY17. This report indicates:
  - Weapon accuracy against stationary land targets has been maintained and moving maritime target accuracy was demonstrated in seven developmental, integrated, and operational free flight test events.
  - JSOW C-1 Mean Flight Hours Between Operational Mission Failure exceeded the requirement value of 95 hours.
  - The Navy has reduced the complexity of the Pilot Vehicle Interface (PVI) in the F/A-18E/F H10 software. There remain minor PVI challenges that could prevent successful mission execution. These challenges can be effectively overcome with proper training prior to employment. The Navy is addressing these challenges in F/A-18E/F H12 Operational Flight Program, scheduled for release in FY17.
  - In operational testing, aircrew workload to employ the weapon increased due to display errors in target location on multiple displays and intermittent errors in the status of the weapon entering the datalink and during post-launch weapon control. The Navy implemented a fix and tested it post-IOC, eliminating these errors.
- Cybersecurity testing of the JSOW C-1 was insufficient to test the cybersecurity vulnerabilities of the weapon and support equipment.

System

- The AGM-154 JSOW family uses a common and modular weapon body capable of carrying various payloads. The JSOW is a 1,000-pound class, air-to-surface glide bomb intended to provide low observable, standoff precision engagement with launch and leave capability. All variants employ a tightly coupled GPS/Inertial Navigation System.
- AGM-154A (JSOW A) payload consists of 145 BLU-97/B combined effects submunitions.
- AGM-154C (JSOW C) utilizes an imaging infrared seeker and its payload consists of an augmenting charge and follow through bomb that can be set to detonate both warheads simultaneously or sequentially.

- AGM-154A and AGM-154C are fielded weapons and no longer under DOT&E oversight. AGM-154C-1 (JSOW C-1) adds moving maritime target capability and the two-way strike common weapon datalink to the baseline AGM-154C weapon.

Mission

- Combatant Commanders use aircraft equipped with JSOW A to conduct pre-planned attacks on soft point and area targets such as air defense sites, parked aircraft, airfield and port facilities, command and control antennas, stationary light vehicles, trucks, artillery, and refinery components.
- Combatant Commanders use aircraft equipped with JSOW C to conduct pre-planned attacks on point targets vulnerable to blast and fragmentation effects and point targets vulnerable to penetration such as industrial facilities, logistical systems, and hardened facilities.
- Combatant Commanders will use F/A-18 E/F aircraft equipped with JSOW C-1 to conduct attacks against moving maritime targets and aircrew will have the ability to retarget weapons post launch. JSOW C-1 will retain the JSOW C legacy capability against stationary land targets.

Major Contractor

Raytheon Company, Missile Systems – Tucson, Arizona

Activity

- The Navy concluded operational testing and declared IOC of the JSOW C-1 in June 2016.
- The Navy completed 166 captive flight test (CFT) runs versus stationary land targets and 160 CFT runs versus mobile maritime targets. However, due to range, target, and environmental limitations as well as a problem with the computer system used to collect the data, many of the planned target runs in the approved operational test plan design of experiments were not accomplished adequately to fully assess

weapon accuracy. The computer system that was used to collect and store the data was unable to produce complete data files for a substantial number of runs against both land and maritime targets. The end-game portions of many runs were missing, resulting in incomplete data files that allowed for the collection of reliability data but not weapon accuracy. The Navy, through follow-on analysis of captive carry test seeker video, was able to assess weapon seeker tracking, but not miss-distance data, for many of the CFT runs.

- The Navy, through follow-on analysis of captive carry test seeker video, was able to assess attack success, but not miss-distance data, on an additional 37 maritime target runs.
- In operational testing, the Navy successfully completed one free flight test event versus a stationary land target on October 21, 2015, and one free flight test versus a mobile maritime target on January 26, 2016.
- The Navy unsuccessfully attempted a free flight test versus a mobile maritime target on February 9, 2016.
  - This shot was designed to be a long-range Advanced Targeting Forward Looking Infrared (AT-FLIR) targeting pod cued shot with handover to a second aircraft for weapon control. Due to range weather limitations, the aircraft providing initial target location and in-flight target updates to the missile was artificially close to the target and passed a very small target location error to the missile to define its search area for the target. However, this aircraft also had an unknown AT-FLIR boresight error, which resulted in a large error in target location. This combination resulted in the target being outside of the missile's search area and a weapon miss. Due to this combination of errors, this event was considered a no-test.
  - A previous captive carry rehearsal of this event on the same sortie, with the aircraft at range providing the initial target location as designed, and without these errors, was assessed as successful.
- The Navy completed carrier suitability testing in February 2016, with 10 catapults and 10 arrestments with aircraft carrying two weapons. The weapons were tested for functionality with no discoveries after this testing.
- Post-IOC, the Navy operational units conducted a live fire Fleet Exercise, Valiant Shield 16, where seven JSOWC-1 weapons were successfully employed against a former Oliver Hazard Perry class frigate. All weapons dropped impacted the ship and achieved high order detonation.
- The Navy conducted cybersecurity testing in April 2016, in accordance with the DOT&E-approved Test and Evaluation Master Plan and operational test plan – except it did not conduct a complete threat representative Adversarial Assessment versus JSOW employment.

Assessment

- DOT&E published a classified FOT&E report in early FY17. This report indicates:
  - Significant amounts of unrecoverable data from captive carry runs, a no-test live fire event, and limited cybersecurity testing resulted in limited information to assess all aspects of JSOW C-1 effectiveness and survivability.
  - Weapon accuracy against stationary land targets has been maintained and moving maritime target accuracy was demonstrated in seven developmental, integrated, and operational free flight test events. .Although the data collected was adequate to demonstrate overall weapon accuracy, it was not adequate to test all the factor effects specified in the approved operational test plan. The additional analysis conducted by the Navy on captive carry test, while unable to gather miss-distance data, was useful in assessing weapon performance and likelihood of attack success.
  - JSOW C-1 Mean Flight Hours Between Operational Mission Failure exceeded the requirement value of 95 hours.
  - The Navy has reduced the complexity of the PVI in the F/A-18E/F H10 software. There remain minor PVI challenges that could prevent successful mission execution. These challenges can be effectively overcome with proper training prior to employment. The Navy has further reduced these challenges in F/A-18E/F H12 software, scheduled for release in FY17.
  - In operational testing, aircrew workload to employ the weapon increased due to display errors in target location on multiple displays, a persistent incorrect advisory of missing cryptographic key data, and intermittent errors in the status of the weapon entering the datalink and during post launch weapon control. The Navy implemented a fix to the Joint Tactical Information Distribution Network Library after the completion of operational testing. This fix was tested during Harpoon II+ testing and in Exercise Valiant Shield with the JSOW; these errors are no longer present.
- Cybersecurity testing of the JSOW C-1 was insufficient to fully test the cyber vulnerabilities of the weapon and support equipment.

Recommendations

- Status of Previous Recommendations. The Navy has partially addressed the previous recommendations. The Navy has demonstrated a reduction in software-driven failures during the extended integrated testing phase. While it has significantly reduced the complex PVI, its plan will not fully address this issue until the F/A-18E/F H12 software release, scheduled for FY17.
- FY16 Recommendations. The Navy should:
  1. Continue to reduce the PVI complexity between the JSOW C-1 and the F/A-18E/F to permit successful mission execution.
  2. Conduct a more complete Cooperative Vulnerability and Penetration Assessment to identify all JSOW and supporting equipment vulnerabilities and a threat-representative Adversarial Assessment, as required by the approved operational test plan.

LHA 6 New Amphibious Assault Ship (formerly LHA(R))

Executive Summary

- LHA 6 completed a 10-month Post Shakedown Availability (PSA) on March 25, 2016. The Navy implemented the changes necessary to incorporate the Joint Strike Fighter (JSF) and the MV-22 Osprey on LHA 6 and will include these changes into the LHA 7 construction plan. LHA 6 will conduct her maiden deployment in mid-2017 with a standard Marine Expeditionary Unit (MEU) Aviation Combat Element (ACE) that includes AV-8B Harrier aircraft. LHA 6 will not complete her operational evaluation of the ship's ability to support a complement of 20 JSF aircraft until FY19.
- The Navy conducted the first part of LHA 6 IOT&E phase OT-C5, which assesses the cybersecurity of the LHA 6. The Cooperative Vulnerability and Penetration Assessment (CVPA) was executed from August 15 – 29, 2016, with the Adversarial Assessment (AA) planned for February 2017. The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted testing on 6 of 128 systems due to limited tester availability, and reported that Hull, Mechanical, and Electrical (HM&E) systems and the Navigation Sensor System Interface (NAVSSI) cannot be tested due to safety concerns.
- The Navy and Marine Corps Operational Test Agencies developed a plan to complete LHA 6 IOT&E phase OT-C4 – the amphibious warfare (AMW) phase – in conjunction with scheduled pre-deployment fleet exercises. The Navy's Program Office is also coordinating with fleet and Marine Corps leadership to conduct the Total Ship Survivability Trial (TSST) in conjunction with these fleet exercises.
- After the PSA, the Navy recommenced LHA 6 IOT&E with the OT-C2 test phase, which was conducted during the Rim of the Pacific multi-national exercise. No Critical Operational Issues were resolved during this phase of test, which was conducted to only provide supplemental data and to inform the Operational Test Agencies as they develop their methodology to execute OT&E in conjunction with the formal certifying fleet exercises in 2QFY17.
- LHA 6 IOT&E phase OT-C3, planned for January 2017, will include tests of the gun systems against the small boat raid and low slow flyer and a demonstration of the chemical warfare detection, protection, and recovery system.
- LHA 6 IOT&E phase OT-C4 will be conducted in April through June 2017. The test will serve as the assessment of the AMW mission areas and be performed in conjunction with the Amphibious Squadron (PHIBRON)/MEU Integration exercise (PMINT), Composite Training Unit Exercise, and conclude with the final Certifying Exercise. Integration of test needs, goals, and requirements is essential from the earliest stage (i.e., the PMINT initial planning conference).

System

- LHA 6 is the lead ship of this new class of large-deck amphibious assault ships designed to support a notional mix of fixed- and rotary-wing aircraft consisting of 12 MV-22 Ospreys, 6 F-35B JSFs (Short Take Off/Vertical Landing variant), 4 CH-53Es, 7 AH 1s/ UH 1s, and 2 embarked H-60 Search and Rescue aircraft, or a load out of 20 F-35Bs and 2 embarked H-60 Search and Rescue aircraft. Key ship features and systems include the following:
  - A greater aviation storage capacity and an increase in the size of the hangar bay is required to accommodate the enhanced aviation maintenance requirements for the MEU ACE with F-35B and MV-22. Additionally, two maintenance areas with high-overhead clearance have been incorporated in the hangar to accommodate maintenance on MV-22s in the spread configuration (wing spread, nacelles vertical, and rotors spread).
  - The ship does not have a well deck. All personnel and equipment transfer to the beach must be done by aviation units.
  - Shipboard medical spaces were reduced by approximately two thirds compared to contemporary LHDs to accommodate the expanded hangar bay.
- The LHA 6 combat system for defense against air threats and small surface craft includes the following major components:
  - The Ship Self-Defense System (SSDS) MK 2 Mod 4B supporting the integration and control of most other combat system elements
  - The ship's AN/SPS-48E and AN/SPS-49A air search radars and the AN/SPQ-9B horizon search radar
  - USG-2 Cooperative Engagement Capability real-time sensor netting system

- The Rolling Airframe Missile and the Evolved Seasparrow Missile (ESSM), with the NATO Seasparrow MK 9 Track Illuminators
- The AN/SLQ-32B(V)2 electronic warfare system with the Nulka electronic decoy-equipped MK 53 Decoy Launching System
- The Phalanx Close-In Weapon System Block 1B and the MK 38 Mod 2 Gun Weapon System
- Two marine gas turbine engines, two electric auxiliary propulsion motors, and two controllable pitch propellers provide propulsion. Six diesel generators provide electric power.
- Command, control, communications, computers, and intelligence (C4I) facilities and equipment support Marine Corps Landing Force operations. The Navy will not install the Consolidated Afloat Networks and Enterprise Services (CANES) on the LHA 6 before FY22, but the LHA 7 design and beyond will deploy with CANES incorporated.
- In addition to the self-defense features discussed above, the ship has the following survivability features:
  - Improved ballistic protection for magazines and other vital spaces as well as the inclusion of some shock hardened systems/components intended to enhance survivability.
  - Various installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from peacetime shipboard fire and flooding casualties and from battle damage incurred during combat.
- The Navy will introduce a Flight 1 variant of the LHA(R) program with the third ship, LHA 8. It will have a well deck for deploying surface connectors to move troops and equipment ashore, a modified flight deck, and reduced island intended to enable an aviation support capability similar to that of LHA 6.

Mission

The Joint Maritime Component Commander will employ LHA 6 to:

- Serve as the primary aviation platform within an Amphibious Ready Group with space and accommodations for Marine Corps vehicles, cargo, ammunition, and more than 1,600 troops
- Serve as an afloat headquarters for an MEU Amphibious Squadron, or other Joint Force commands using its C4I facilities and equipment
- Accommodate elements of a Marine Expeditionary Brigade when part of a larger amphibious task force
- Carry and discharge combat service support elements and cargo to sustain the landing force

Major Contractor

Huntington Ingalls Industries, Ingalls Shipbuilding Division – Pascagoula, Mississippi

---

Activity

- LHA 6 completed her PSA on March 25, 2016. The 10-month long PSA, held from May 2015 until March 2016, prevented any significant testing through the availability. The principal tasks accomplished during PSA were the design modifications to the flight deck to account for the deck strengthening, heat-resistant material improvements, and lighting positioning to accommodate the JSF F-35B and benefit MV-22 Osprey operations. The flight deck changes have been included in the LHA 7 design currently under construction at Huntington Ingalls shipyard.
- Since completing her PSA, the Navy recommenced LHA 6 IOT&E with the OT-C2 test event, conducted from June 29 through August 3, 2016. The test was conducted during the Rim of the Pacific multi-national exercise. No Critical Operational Issues were resolved during this phase of test. The exercise was conducted to provide supplemental data and to develop a methodology on how best to accomplish testing in conjunction with the formal certifying fleet exercises to be conducted in 2QFY17.
- The Navy conducted the LHA 6 cybersecurity testing CVPA from August 15 – 29, 2016, and the AA is planned for February 2017. COTF conducted testing on 6 of 128 systems, but did not perform testing on HM&E systems due to safety concerns. The Navy did not permit any hands-on manipulation of HM&E or NAVSSI systems; the Navy plans to construct a stand-alone laboratory environment to conduct testing of such shipboard systems in high fidelity representative test environments without the risk of corrupting them..
- The Navy is developing an LHA(R) Test and Evaluation Master Plan (TEMP) Revision B to address design modifications to LHA 8, including the addition of the well deck and changes to the flight deck, the island configuration, the combat system, medical spaces, fuel tanks, and supporting spaces. Evolutions of Marine Corps aircraft, surface connectors, and vehicles will also be considered.
- The Navy has stated it is not planning to execute the Advanced Mine Simulation System (AMISS) trial, which would be used to establish the mine susceptibility of the LHA 6, as agreed to in the DOT&E-approved TEMP Revision A. To date, the Navy has not presented a valid alternative to conducting the AMISS trial.

Assessment

- Because LHA 6 does not have a well-deck, it will rely exclusively on air assets to move forces ashore. The Navy and Marine Corps are in the process of adjusting their tactics to be consistent with the capabilities of LHA 6. In particular, the aircraft mix and equipment load-out used on an LHD with a well deck is unlikely to enable combat power to be massed rapidly ashore from LHA 6. The Navy and Marine Corps to date have not finalized the tactics that will be required for IOT&E.

- The LHA 6 TSST, which contributes to the survivability assessment of the ship, was planned to occur during the AMW event consistent with execution of an efficient test program. The Navy has rescheduled the test to occur before the LHA 6 pre-deployment exercises in March/April 2017 to ensure the presence of an operationally representative load-out aboard the ship during the TSST. The Navy has coordinated with the fleet and Marine Corps leadership to ensure the TSST is conducted in an operationally realistic manner.
- Results of testing completed to date continue to indicate that LHA 6 has some ship self-defense capability against older ASCM threats. LHA 6 ship self-defense performance against newer ASCM threats remains undetermined pending completion of the Probability of Raid Annihilation modeling and simulation test bed tests for IOT&E in late 2017.
  - The Navy initiated the Fire Control Loop Improvement program (FCLIP) to correct some combat system deficiencies related to self-defense against ASCMs and has the potential to mitigate some of the vulnerabilities.
  - The Navy has completed Phase 1 of the FCLIP. What was formally known as FCLIP Phase 2 and 3 are now merged into FCLIP Phase 2, which is not funded. Absent full funding of FCLIP, significant deficiencies will remain in the ability of the ship to defend itself against threats proliferating worldwide.
- DOT&E does not agree that the Navy's proposed modeling and simulation-based approach to assessing the mine susceptibility of LHA 6 is adequate. The Navy should plan to execute the AMISS trial as agreed to in the DOT&E-approved TEMP Revision A.

Recommendations

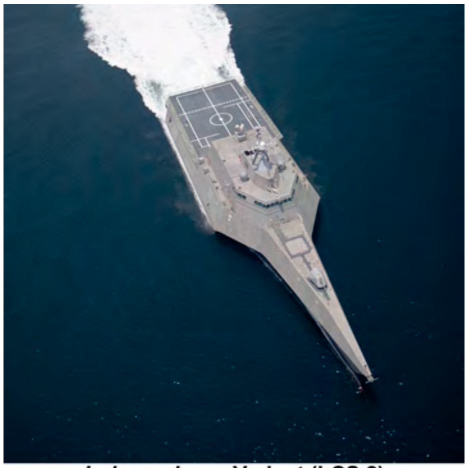
- Status of Previous Recommendations. The Navy:
  1. Has not fully resolved the recommendation to correct systems engineering deficiencies related to SSDS MK 2-based combat systems and other combat system deficiencies so that LHA 6 can satisfy its Probability of Raid Annihilation requirement.
  2. Has not yet resolved the MK 29 launcher system motor failures due to the additional weight of the ESSM.
  3. In conjunction with the Marine Corps, finalize the tactics, techniques, and procedures for LHA 6 prior to the phase of IOT&E in which they will be used.
  4. Has neither planned nor resourced the mine susceptibility trial for the LHA 6 using the AMISS.
- FY16 Recommendations. The Navy should:
  1. Conduct cybersecurity testing of HM&E and Navigation systems, which was deferred due to safety concerns, in a laboratory to understand the systems' vulnerabilities.
  2. Fully fund and execute all phases of the FCLIP.
  3. Execute the AMISS trial as agreed in TEMP Revision A.

Littoral Combat Ship (LCS)

Executive Summary

- Over the last year, DOT&E published four reports on the LCS program:
  - An assessment of the results of operational testing of the *Freedom*-variant seaframe equipped with the Increment 2 surface warfare (SUW) mission package (December 2015)
  - A response to satisfy Congressional reporting requirements in the National Defense Authorization Act (NDAA) for FY16 (January 2016)
  - An early fielding report that provided DOT&E's interim assessments of operational effectiveness and suitability of the *Independence*-variant LCS equipped with the mine countermeasures (MCM) mission package (June 2016)
  - An assessment of the results of operational testing of the *Independence*-variant seaframe equipped with the Increment 2 SUW mission package (November 2016)
- The ability of LCS to perform the bulk of its intended missions (SUW, MCM, and anti-submarine warfare (ASW)) depends on the effectiveness of both the host seaframe and the installed mission packages. To date, despite LCS having being in service since 2008, the Navy has not yet demonstrated effective capability for LCS equipped with the MCM, SUW, or ASW mission packages.
  - As one of the results of a failed technical evaluation period in 2015, the Navy canceled the Remote Minehunting System (RMS), a core component of the MCM mission package. Therefore, the MCM mission package will be unable to meet the Navy's minehunting requirements until replacement systems can demonstrate operationally effective and suitable capabilities, which will not occur before 2020. Mine neutralization and sweeping systems also have yet to demonstrate operationally effective and suitable capabilities in the MCM mission package.
  - The ASW mission package continues to undergo development and is not expected to be ready for operational testing on the first seaframe until 2018 at the earliest.
  - The Increment 2 SUW mission package, following a 2014 operational test aboard a *Freedom* variant and a 2016 operational test aboard an *Independence* variant, has demonstrated only modest ability to aid the ship in defending itself against small swarms of small boats, and the ability to support maritime security operations. The Navy has not yet demonstrated in an operational test that an LCS equipped with this mission package has an offensive capability, such as in an escort mission (a traditional frigate role), nor the capability to defend itself against threat-representative numbers and tactics of attacking small boats. The Navy believes it will meet the original LCS SUW requirements with the introduction of Increment 3 of the SUW mission package, scheduled to begin operational testing in FY18.

Freedom **Variant (LCS 1)**



Independence **Variant (LCS 2)**

  - In September 2016, the Navy announced actions being taken to implement the recommendations of the LCS review team established in February. LCS program changes will reportedly include semi-permanent installation of mission package systems in the seaframes, dedicating specific ships to specific missions. The Navy originally designed LCS from the outset as a "seaframe" into which interchangeable mission packages could be installed. The change represents a departure from the Navy's original concept that intended to provide the Maritime Component Commander with the flexibility to interchange modular capability on any LCS seaframe, as required by the mission. Twenty-four of the planned 28 ships will form into six divisions with three divisions on each coast – *Independence* variants on the west coast and *Freedom* variants on the east coast. Each division of four ships will have a single warfare focus and the crews and mission module detachments will be combined.
- In response to conditions that the NDAA for FY16 placed on the availability of LCS program funding, the Navy successfully completed a partial update of the LCS Test and Evaluation Master Plan (TEMP) to support future operational test and evaluation of the seaframes and mission packages.

Congress required the update to support planning of the needed testing of the Increment 3 SUW mission package, the ASW mission package, to reflect the significant changes to the program's air defense plans, as well as MCM mission package development and composition. DOT&E approved the TEMP change pages submitted by the Navy in March 2016. The Navy is now working to complete a full revision of the TEMP.

- **Live Fire.**
  - The LCS 4 Total Ship Survivability Trial (TSST), conducted in January 2016, exposed weaknesses in the *Independence*-variant design. While the shock-hardened auxiliary bow thruster would have provided limited post-shock propulsion, much of the ship's mission capability would have been lost because critical support systems (such as chilled water) are not designed for reconfiguration and isolation of damage caused by the initial weapons effects or caused by the ensuing fire and flooding.
  - In June and July 2016, the Navy conducted a reduced severity shock trial on USS *Jackson* (LCS 6), executing three shots of increasing severity, ending at 50 percent of the maximum design level rather than 67 percent as done on other ship classes.
    - The Navy argued the reduced severity approach taken for LCS 6 was necessary because it lacked specific test data and a general understanding of how the non-hardened systems would respond to shock. To further mitigate potential equipment damage and personnel injury, some mission systems were removed, other equipment was modified to improve its shock resistance, and construction deficiencies were corrected.
    - The electrical distribution system remained operable or was restored to a limited or full capability prior to the ship's return to port after each shot.
    - Most non-hardened components and systems, including the SeaRAM air defense system, remained operable or were restored to a limited or full capability prior to the ship's return to port after each shot. The Navy is still analyzing the structural response data.
    - DOT&E will release a more comprehensive report in 2017 upon complete analysis of the trial data.
  - Based on the LCS 6 shock trial lessons learned, the Navy conducted a shock trial aboard USS *Milwaukee* (LCS 5) from August 29 through September 23, 2016, starting the trial at more traditional severity levels. However, the Navy stopped the LCS 5 trial after the second shot due to concerns with the shock environment, personnel, and equipment. The Navy did not view the third LCS 5 shock event as worthwhile because of concerns that shocking the ship at the increased level would significantly damage substantial amounts of non-mission-critical equipment, as well as significantly damage a limited amount of hardened, mission-critical equipment, thereby necessitating costly and lengthy repairs.
    - DOT&E cannot adequately assess the survivability of the *Freedom* variant to underwater shock threats, although the behavior of the ship was better than expected throughout the two executed events.
    - Most non-hardened components and systems, including electrical power generation systems and the RAM air defense system, remained operable or were restored to a limited or full capability prior to the ship's return to port after each shot.
    - By not executing the 2/3 level shot, the Navy could not validate the overly conservative assumptions made for the underwater threat shot in the LCS 3 TSST.
    - DOT&E will release a more comprehensive classified report in 2017 upon complete analysis of the trial data.
- **Air Defense.**
  - In June 2016, the Navy responded to DOT&E's August 2015 memorandum that advised the Navy to adopt an alternative test strategy for air defense testing given the Navy's inability to obtain the intellectual property necessary to develop high-fidelity models of the ships' radars. In its response, the Navy indicated that it does not plan to test the current configuration of the *Freedom* variant's air defense system. Instead, the Navy plans to replace the *Freedom* variant's Rolling Airframe Missile (RAM) system with the SeaRAM system starting on LCS 17 and follow-on ships of that variant and will conduct the appropriate testing of that system at the appropriate time. The Navy plans to backfit SeaRAM onto the earlier ships of that variant (LCS 1 through 15) in the 2020-2025 time period. Thus, there will be a 5-10 year gap during which the effectiveness of the deployed *Freedom* variants' air defense system will remain unknown and untested, leaving sailors without knowledge of the capabilities and limitations of their systems should they come under attack.
  - Also in June 2016, the Navy postponed indefinitely its plans to conduct the first of four live fire test events aboard the self-defense test ship to examine the effectiveness of the *Independence* variant's SeaRAM air defense system, citing initial modeling predictions that predicted poor performance in the planned test event scenario. In July 2016, the LCS Program Executive Officer sent a letter to the Navy's Surface Warfare Director (N96) stating that the *Independence* variant's air warfare testing directed by the extant TEMP cannot be executed at current funding levels. DOT&E expects that the *Independence* variant will have been in service nearly 10 years by the time that air defense testing is complete, which at the time of this report, is not anticipated before FY20.
- **Surface Warfare.** While equipped with the Increment 2 SUW mission package, LCS 4 participated in three engagements with small swarms of small boats in the 2015-2016 operational test period. LCS 4 failed the Navy's reduced requirement for interim SUW capability, failing to defeat each of the small boats before one penetrated the prescribed keep-out zone in two of the three events. Although LCS eventually destroyed or disabled all of the attacking boats in these events, the operational test results suggest that the Increment 2 SUW mission package provides the crew with a moderately

enhanced self-defense capability (relative to the capability of the seaframe's 57 mm gun alone), but not an effective offensive capability. In all three events, the ship expended an inefficiently large quantity of ammunition from the 57 mm gun and the two mission package 30 mm guns, while contending with azimuth elevation inhibits that disrupted or prevented firing on the targets. In one event, frequent network communication faults disrupted the flow of navigation information to the gun systems, further hindering the crew's efforts to defeat the attacking boats. LCS 4's failure to defeat this relatively modest threat routinely under test conditions raises questions about its ability to deal with more realistic threats certain to be present in theater, and suggests that LCS will be unsuccessful operating as an escort (a traditional frigate role) to other Navy ships.

- **Seaframe Suitability.** DOT&E has now evaluated both seaframe variants to be not operationally suitable because many of their critical systems are unreliable, and their crews do not have adequate training, tools, and documentation to correct failures when they occur. No matter what mission equipment is loaded on either of the ship variants, the low reliability and availability of seaframe components, coupled with the small crew size, imposed significant constraints on mission capability. During this last year, the seaframes encountered multiple problems with main engines, waterjets, communications, air defense systems, and cooling for the combat system. Unless corrected, the critical operational suitability problems highlighted in this report as well as multiple DOT&E test reports will continue to prevent the ship and mission packages from being operationally effective.
- **Mine Countermeasures.** After canceling the RMS program, the Navy announced its intention to evaluate alternatives to the RMS such as an unmanned surface craft towing improved minehunting sensors and the Knifefish unmanned undersea vehicle (UUV). Although the Navy intended to accelerate development of Knifefish pre-planned product improvements, that effort was not funded. The Navy abandoned plans to conduct operational testing of individual MCM mission package increments and delayed the start of the LCS MCM mission package IOT&E on the first seaframe until late FY20. The Navy also delayed the IOT&Es of the LCS-based airborne mine countermeasures (AMCM) systems that it had expected to complete in FY16 during the operational test of the LCS with the first increment of the MCM mission package.
- **Over-the-Horizon Missile.** The Navy is preparing to add an over-the-horizon anti-ship missile capability to in-service LCS seaframes before they deploy, as soon as FY17. To date, the Navy has completed two structural test firing events from an *Independence*-variant seaframe using two different candidate missile systems. These tests were conducted to determine whether the installed missile systems carry any risk of damaging the ship's structure. A Naval Strike Missile was fired from LCS 4 in September 2014, and a Harpoon Missile was fired from LCS 4 during 2016's Rim of the Pacific (RIMPAC) exercise. The Navy has not conducted any further developmental testing of either missile system, and neither missile has been exercised during an LCS operational test.
- **Cybersecurity.** In early 2016, the Navy made substantial changes to the LCS 4's networks, calling the effort "information assurance (IA) remediation," to correct many of the deficiencies in network security in the baseline *Independence* variant's total ship computing environment. The Navy's IA remediation corrected some of the most severe deficiencies known prior to the test period. However, testing revealed that several problems still remain which will degrade the operational effectiveness of *Independence*-variant seaframes until the problems are corrected. The Navy plans a second phase of IA remediation to correct additional network deficiencies.

System

Seaframes

- The LCS is designed to operate in the shallow waters of the littorals that limit the access of larger ships.
- The Navy is currently procuring two LCS seaframe variants:
  - The *Freedom* variant (odd-numbered ships) is a semi-planing monohull design constructed of steel (hull) and aluminum (deckhouse) with two steerable and two fixed-boost water jets driven by a combined diesel and gas turbine main propulsion system.
  - The *Independence* variant (even-numbered ships) is an aluminum trimaran with two steerable water jets driven by diesel engines and two steerable water jets driven by gas turbine engines.
- Common design specifications include:
  - Sprint speed in excess of 40 knots, draft of less than 20 feet, and an unrefueled range in excess of 3,500 nautical miles at 14 knots
  - Accommodations for up to 98 personnel
  - A common Mission Package Computing Environment for mission package control using Mission Package Application Software installed when a mission package is embarked
  - A Multi-Vehicle Communications System to support simultaneous communications with multiple unmanned off-board vehicles
  - Hangars sized to embark MH-60R/S and Vertical Take-off Unmanned Aerial Vehicles (VTUAVs)
  - MK 110 57 mm gun (BAE/BOFORS)
- The variants include the following damage control features:
  - Ballistic protection for magazines and other vital spaces
  - Various installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from shipboard fire and flooding casualties
- The designs have different core combat systems to provide command and control, situational awareness, and self defense against anti-ship cruise missiles (ASCMs) and surface craft.
  - *Freedom* variant: COMBATSS-21, an Aegis-based integrated combat weapons system with a TRS-3D (AN/SPS-75) air and surface search radar (ASR) (Airbus, France); Rolling Airframe Missile (RAM) system supported by elements from the Ship Self Defense System (Raytheon) (one 21-cell launcher); a Terma Soft

Kill Weapon System (Denmark); and a DORNA EOD gunfire control system with an electro optical/infrared sensor (Navantia, Spain) to control the MK 110 57 mm gun. In 2013 the Navy announced that, starting with LCS 17, future *Freedom*-variant ships will be fitted with SeaRAM, instead of RAM, as their air defense system. The Navy is also developing plans to backfit SeaRAM on earlier *Freedom* seaframes between 2020 and 2025. In the interim, the Navy has accepted the operational risk associated with continued operation of *Freedom* seaframes with the RAM air defense system, and does not plan to operationally test this configuration.
  - *Independence* variant: Integrated Combat Management System derived from the Thales TACTICOS system (The Netherlands) with a Sea Giraffe (AN/SPS-77) ASR (SAAB, Sweden); one MK 15 Mod 31 SeaRAM system (Raytheon) (integrates the search, track, and engagement scheduler of the Phalanx Close-in Weapon System with an 11-round RAM launcher assembly); Automatic Launch of Expendables (ALEX) System (off-board decoy countermeasures) (Sippican, U.S.), and SAFIRE (FLIR, U.S.) for 57 mm gun fire control.
- Commencing with LCS 7 and LCS 10, the Navy plans to incorporate changes needed for compatibility with the ASW mission package in future seaframes. The Navy has not yet addressed the plan for backfitting these changes in earlier seaframes.
- The Navy is preparing to add an over-the-horizon anti-ship missile capability to in-service LCS seaframes before they deploy, as soon as FY17. To date, the Navy has completed two structural test firing events from an *Independence* variant seaframe using two different candidate missile systems: the Naval Strike Missile System (Kongsberg/Raytheon) and the Harpoon weapon system (Boeing).
- The Navy originally planned to acquire 55 LCSs, but reduced the planned procurement to 52 ships in 2013. In a February 24, 2014, memorandum, the Secretary of Defense announced that no new contract negotiations beyond 32 ships would go forward and directed the Navy to submit alternative proposals to procure a more capable and lethal small surface combatant, generally consistent with the capabilities of a Frigate. In December 2015, the Secretary of Defense directed that the total procurement of LCS and the improved small surface combatant variant (now called a Frigate) be truncated to 40 ships. The Secretary also directed that the LCS program down-select to a single variant and transition to the Frigate no later than FY19. The Navy plans to acquire the last 12 ships in the Frigate configuration, for which the two prime contractors are developing proposals.

Mission Packages
- LCS is designed to host a variety of individual warfare systems (mission modules) assembled and integrated into interchangeable mission packages. The Navy currently plans to field MCM, SUW, and ASW mission packages. A mission package provides the seaframes with capability for a single or "focused" mission. Multiple individual programs of record involving sensor and weapon systems and off-board vehicles make up the individual mission modules. Summarized below is the current acquisition strategy for the incremental development of each mission module. Although the Navy had been planning to field four increments of the MCM mission package following associated phases of operational testing, the program has recently decided to integrate and field new capabilities whenever they are ready. The Navy also deferred IOT&E of the MCM mission package until mine hunting and sweeping systems are mature enough to complete end-to-end mine clearance requirements throughout most of the water column.

SUW Mission Package
- Increment 1 included:
  - Gun Mission Module (two MK 46 30 mm guns)
  - Aviation Module (embarked MH-60R/S). Because of a shortage of MH-60R helicopters, the Navy is substituting the less-capable MH-60S helicopter, which does not have a radar.
- Increment 2 added:
  - Maritime Security Module (two 11-meter rigid-hull inflatable boats (RHIBs) with associated launch and recovery equipment)
- Increment 3 will add:
  - Surface-to-Surface Missile Module (SSMM) Increment I, employing the AGM 114L-8A Longbow HELLFIRE missile
  - One MQ-8B or MQ-8C Fire Scout VTUAV to augment the Aviation Module
- Increment 4, if fielded, would add:
  - SSMM Increment II (replacing Increment I) to provide a longer range surface engagement capability

MCM Mission Package
- The current version of the mission package (formerly described as Increment 1) includes:
  - Remote Minehunting Module, consisting of two Remote Multi-Mission Vehicles (RMMVs) (version 6.0) and three AN/AQS-20A sensors.
  - Aviation Module consisting of an MH-60S Block 2B or subsequent AMCM helicopter outfitted with an AMCM system operator workstation and a tether system.
  - Near Surface Detection Module, consisting of one Airborne Laser Mine Detection System (ALMDS) and an embarked spare.
  - Airborne Mine Neutralization Module, consisting of one Airborne Mine Neutralization System (AMNS) unit and an embarked spare. The current version of AMNS does not include a near-surface mine neutralization capability.
- The composition of the future (circa FY20-25) MCM mission package is unsettled. In the wake of the Navy's Technical Evaluation of the current mission package in 2015, an independent review team recommended that the Navy cancel plans to procure additional RMMVs and instead evaluate other alternatives. The Navy subsequently canceled the RMS program but funded refurbishment of a

small number of the existing RMMVs. Although the Navy may still employ the existing RMMVs in some capacity, planning for developmental and operational testing of the mission package is proceeding under the assumption that the future minehunting capability will be provided by one or two unmanned surface vessels towing an AN/AQS-20C or AN/AQS-24C minehunting sensor and a pair of Knifefish UUVs. Both minehunting solutions are under development.

- In addition to the selected minehunting system and the AMCM systems ALMDS and AMNS, for which the Navy plans to declare Initial Operational Capability (IOC) in FY17, the future MCM mission package will likely include:
  - Coastal Mine Reconnaissance Module, consisting of the Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I, Block II, or Block III system and one MQ-8B or MQ-8C VTUAV for daytime unmanned aerial tactical reconnaissance to detect and localize mine lines and obstacles in the beach zone (Blocks I and II) and the surf zone (Block II). The Navy also expects the Block II system to add improved beach zone detection capability against small mines and add nighttime capability. As currently envisioned, Block III will add the capability to detect buried mines in the beach zone and surf zone. The Navy expects the Block I system to reach IOC in FY17. The Navy expects Block II to reach IOC in FY22; the Block III IOC date has not yet been established.
  - An Unmanned Mine Sweeping Module, consisting of the Unmanned Influence Sweep System (UISS) to detonate acoustic-, magnetic-, and combined acoustic/magnetic-initiated volume and bottom mines. The Navy is developing an unmanned surface vehicle (USV) based on the UISS surface craft that can host the minesweeping system or tow a minehunting sensor. The Navy expects UISS to reach IOC early in FY19.
  - The Barracuda Mine Neutralization System (MNS), which the Navy expects to provide a near-surface mine neutralization capability. If successful, it will also augment AMNS in other portions of the water column. The Navy plans to deploy Barracuda from LCS using the USV as well as manned and unmanned aircraft and expects the system to be ready to begin developmental testing in FY22.
  - Buried Minehunting Module, consisting of two Knifefish UUVs, battery-powered, autonomous underwater vehicles, employing a low frequency, broadband, synthetic aperture sonar to detect and classify volume and bottom mines in shallow water. The Navy plans for Knifefish to reach IOC in FY18.
  - Pre-planned product improvements (P3I) to ALMDS are currently unfunded. When funding becomes available, the Navy also plans to commence developmental testing of an alternate AMNS fiber-optic cable material designed to reduce the incidence of breakage.
- The Navy is planning to use Expeditionary MCM units – consisting of Explosive Ordnance Disposal personnel equipped with legacy MCM systems and experimental systems deployed to theater – to augment LCSs equipped with MCM mission packages. In particular, the Navy envisions Expeditionary MCM forces, aboard LCSs or other ships, as a gap-filler in missions for which LCS MCM mission package capabilities do not yet exist.

ASW Mission Package

- Torpedo Defense and Countermeasures Module (Lightweight Tow torpedo countermeasure)
- ASW Escort Module (Multi-Function Towed Array and Variable Depth Sonar)
  - The Navy expects to select the vendor for these systems in FY17 and conduct the first operational test of the ASW mission package in late FY18.
- Aviation Module (embarked MH-60R and MQ-8B or MQ-8C Fire Scout VTUAV)

Mission

- The Maritime Component Commander will employ LCS to conduct MCM, ASW, or SUW tasks depending on the mission package installed in the seaframe. Because of capabilities inherent to the seaframe, commanders can employ LCS in a maritime presence role in any configuration. With the Maritime Security Module, installed as part of the SUW mission package, the ship can conduct Maritime Security Operations, including Visit, Board, Search, and Seizure of ships suspected of transporting contraband.
- In September 2016, the Navy announced actions being taken to implement the recommendations of the LCS review team established in February. LCS program changes will reportedly include semi-permanent installation of mission package systems in the seaframes, dedicating specific ships to specific missions. The Navy originally designed LCS from the outset as a “seaframe” into which interchangeable mission packages could be installed. The change represents a departure from the Navy’s original concept that intended to provide the Maritime Component Commander with the flexibility to interchange modular capability on any LCS seaframe, as required by the mission. Twenty-four of the planned 28 ships will form into six divisions with three divisions on each coast – *Independence* variants on the west coast and *Freedom* variants on the east coast. Each division of four ships will have a single warfare focus and the crews and mission module detachments will be combined.
- The Navy can employ LCS alone or in company with other ships. The Navy’s Concept of Operations (CONOPS) for LCS anticipates that the ship’s primary operational role will involve preparing the operational environment for joint force assured access to critical littoral regions by conducting MCM, ASW, and SUW operations, possibly under an air defense umbrella as determined necessary by the operational commander. However, the latest CONOPS observes, “The most effective near-term operational roles for LCS to support the maritime strategy are theater security cooperation and maritime security operations supporting deterrence and maritime security.”

Major Contractors

- *Freedom* variant
  - Prime: Lockheed Martin Maritime Systems and Sensors – Washington, District of Columbia
  - Shipbuilder: Marinette Marine – Marinette, Wisconsin
- *Independence* variant
  - Prime for LCS 2 and LCS 4: General Dynamics Marine Systems Bath Iron Works – Bath, Maine
  - Prime for LCS 6 and subsequent even numbered ships: Austal USA – Mobile, Alabama
  - Shipbuilder: Austal USA – Mobile, Alabama
- Mission Packages
  - Mission Package Integration contract awarded to Northrop Grumman – Los Angeles, California

---

Activity

LCS Program

- In December 2015, DOT&E published an assessment of the results of operational testing of the *Freedom*-variant seaframe equipped with the Increment 2 SUW mission package.
- In January 2016, DOT&E responded to the reporting requirement in section 123 of the NDAA for FY16, which directed DOT&E to report to Congress and the Secretary of Defense on the current CONOPS and expected survivability attributes of each of the seaframes. This report was an update to similar reporting requirements in both the NDAAs for FY14 and FY15. DOT&E tailored this report to address changes to previous assessments due to the additional testing conducted following the previous years' submissions.
- In February 2016, the Chief of Naval Operations and the Assistant Secretary of the Navy for Research, Development, and Acquisition established a panel headed by the Commander, Naval Surface Forces to review the LCS program, including the crewing, operations, training, and maintenance of the ships.
- In response to conditions that the FY16 NDAA placed on the availability of LCS program funding, the Navy successfully completed a partial update of the LCS TEMP to support future OT&E of the seaframes and mission packages. Congress required the update to support planning of the needed testing of the Increment 3 SUW mission package, the ASW mission package, to reflect the significant changes to the program's air defense plans, as well as MCM mission package development and composition. DOT&E approved the change pages to the TEMP in March 2016. Additional updates are required to complete a revision to the TEMP, including developmental and integrated testing plans, changes to reflect the Navy's evolving plans for the MCM mission package, air defense testing of the seaframes, and plans for providing seaframes with an over-the-horizon missile capability.
- In April 2016, DOT&E provided USD(AT&L) an assessment of the capabilities and limitations of LCS ships and mission packages to support USD(AT&L)'s FY16 annual in-process review of the LCS program. That report summarized DOT&E's current assessment of both LCS variants, including an evaluation of the seaframes' cybersecurity, air defense, surface self-defense, reliability, and availability, and known survivability shortfalls. The report also provided a preliminary assessment of recent developmental and operational test results in advance of the formal submission of operational test and early fielding reports for the SUW and MCM mission packages, respectively.
- In June 2016, DOT&E submitted an early fielding report to the Congress in response to the Navy's plan to deploy the *Independence*-variant LCS equipped with the MCM mission package prior to the conduct of operational testing. The classified report provided DOT&E's interim assessments of operational effectiveness and operational suitability of the *Independence*-variant LCS employing the MCM mission package consisting of the RMS, MH-60S, ALMDS, and AMNS.
- In September 2016, the Navy announced actions being taken to implement the recommendations of the LCS review team established in February. LCS program changes will reportedly include semi-permanent installation of mission package systems in the seaframes, dedicating specific ships to specific missions. The Navy originally designed LCS from the outset as a "seaframe" into which interchangeable mission packages could be installed. The change represents a departure from the Navy's original concept that intended to provide the Maritime Component Commander with the flexibility to interchange modular capability on any LCS seaframe, as required by the mission. Twenty-four of the planned 28 ships will form into six divisions with three divisions on each coast – *Independence* variants on the west coast and *Freedom* variants on the east coast. Each division of four ships will have a single warfare focus and the crews and mission module detachments will be combined. The Navy also plans to establish "maintenance execution teams" staffed with LCS sailors in each division to assist ship crews with preventive and corrective maintenance. One of the ships in each division will be a dedicated training platform; it will not normally deploy overseas and will be staffed by a single crew of experienced LCS sailors. The Navy plans to adopt the blue-gold crewing model (two crews for every one ship) for selected ships instead of the current 3-2-1 crewing plan, which provides three crews for every two ships to keep one of those ships forward deployed. The Navy also plans to dedicate the

first four LCSs for experimentation, test, and evaluation activities vice routinely deploying them as part of the normal ship deployment rotation.

- In November 2016, DOT&E published an assessment of the results of operational testing of the *Independence*-variant seaframe equipped with the Increment 2 SUW mission package.

Seaframe Test Activities

- *Freedom* Variant:
  - During high-speed operations aboard LCS 5 in December 2015, a software failure resulted in damage to the high-speed clutches connecting the gas turbine engines to the combining gears, contaminating the lubricating oil system and damaging the combining gears. Repairs to the clutches and combining gears sidelined the ship for about 3 months.
  - In January 2016, during diesel engine testing aboard LCS 3 at the Changi Naval Base in Singapore, combining gears were damaged when they were operated without lubrication. After a lengthy repair period, the ship departed Singapore for San Diego, California, on August 22, 2016, having been out of service for more than 6 months.
  - In June 2016, the Navy responded to DOT&E's August 2015 memorandum that advised the Navy to adopt an alternative test strategy for air defense testing given the Navy's inability to obtain the intellectual property necessary to develop high-fidelity models of the ships' radars. The Navy's response indicated the Navy does not plan to test the current configuration of the *Freedom* variant's air defense system. Instead, the Navy plans to install the SeaRAM system on LCS 17 and beyond and will conduct the appropriate testing of that system at the appropriate time. The Navy plans to backfit SeaRAM onto the LCS 1-15 hulls in the 2020-2025 time period. This plan reveals a 5-10 year gap where the effectiveness of the deploying *Freedom* variants' air defense system remains unknown and untested.
  - The Navy reported that LCS 1, serving as an Afloat Forward Staging Base, demonstrated the ability to conduct Expeditionary MCM operations during the biennial Rim of the Pacific (RIMPAC) exercise in July 2016. DOT&E has not yet been provided details on these exercises.
  - During the same time period, LCS 1 returned to port multiple times to effect repairs, including decontamination of the lube oil system to remove seawater. Following LCS 1's participation in RIMPAC, the Navy reported that an investigation of the ship's propulsion plant revealed significant damage to at least one of the engines caused by rust and seawater and that it will be necessary to replace or rebuild the engine.
  - The Navy conducted a two shot shock trial aboard USS *Milwaukee* (LCS 5) from August 29 through September 23, 2016.
- *Independence* Variant:
  - The Navy executed a Total Ship Survivability Trial (TSST) aboard USS *Coronado* (LCS 4) from January 25 – 28, 2016.
  - From June 7 to July 17, 2016, the Navy conducted a three shot reduced-severity shock trial of USS *Jackson* (LCS 6) off the eastern coast of Florida.
  - From September 2015 until July 2016, the Navy performed blast and fire testing on the Multi-Compartment Surrogate (MCS) at Aberdeen Proving Grounds, Maryland to assess the vulnerability of the welded-aluminum ship structures under internal blast loading and fire exposure. The Navy will also use these data to update the modeling and simulation tools used in the survivability evaluation of the *Independence* variant.
  - Because of changes to the ship's air defense system, SeaRAM, and additional modifications to the ship's combat system and networks (referred to as IA remediation), the Navy conducted additional testing of the Increment 2 version of the SUW mission package and *Independence*-variant seaframe from March through June 2016. These test events included:
    - Previously deferred developmental test events
    - Air defense testing to examine radar tracking performance against subsonic aerial drones
    - Cybersecurity testing
    - A single self-defense live-fire event and multiple tracking events to confirm that the changes did not degrade SUW performance
  - In December 2015, the Navy conducted the first operationally realistic live-fire event aboard the self-defense test ship, where the SeaRAM system was successful at defeating a raid of two GQM-163 supersonic targets.
  - In June 2016, LCS 4 conducted its second shipboard live fire of the ship's SeaRAM system against a single subsonic aerial drone. The live-fire demonstration was not designed to be an operationally realistic test of the ship's capability, and the aerial drone's flight profile and configuration were not threat representative. These tests provide no insight into SeaRAM's effectiveness against threats that LCS is likely to encounter, but they confirmed that SeaRAM is able to at least target and launch RAM missiles – a necessary but not sufficient testing milestone.
  - During the 2015-2016 operational testing aboard LCS 4, the Navy conducted several non-firing events to examine components of the *Independence* variant's air defenses. These included non-firing radar tracking events against subsonic ASCM drones (June 2016), and non-firing tracking events against Learjet aircraft equipped with ASCM seeker simulators ES-3601 (to test the electronic support measures (ESM) system) (September 2015). The Navy failed to execute a test of the ship's capability to track tactical aircraft in both clear and jamming environments. Such a test was scheduled to occur during

the FY16 operational test events; it is now rescheduled for January 2017.
- In June 2016, the Navy postponed indefinitely its plans to conduct the first of four live fire test events aboard the self-defense test ship to examine the effectiveness of the *Independence* variant's SeaRAM air defense system, citing initial modeling predictions that predicted poor performance. In July 2016, the LCS Program Executive Officer sent a letter to the Navy's Surface Warfare Director (N96) stating that *Independence* air warfare testing directed by the extant LCS TEMP cannot be executed at current funding levels.
- The Navy is preparing to add an over-the-horizon anti-ship missile capability to in-service LCS seaframes before they deploy, as soon as FY17. To date, the Navy has completed two structural test firing events from an *Independence*-variant seaframe using two different candidate missile systems. These tests were conducted to determine if the installed missile systems carry any risk of damaging the ship's structure. A Naval Strike Missile was fired from LCS 4 in September 2014, and a Harpoon Missile was fired from LCS 4 during the July 2016 RIMPAC exercise. The Navy has not conducted any further developmental testing of either missile system, and neither missile has been exercised during an LCS operational test.
- LCS 4 deployed to the western Pacific following participation in RIMPAC, but returned to Pearl Harbor under escort in late August because of a propulsion system casualty that resulted in the failure of two high-speed flexible couplings. LCS 4 was supposed to replace LCS 3 as the rotationally deployed LCS in Singapore. The Navy evaluated the damage and determined this casualty was not a result of human error, but rather a material deficiency. The Navy completed the necessary repairs to the two high-speed flexible couplings and LCS 4 resumed its deployment in late-September.
- After operating out of Pensacola, Florida, for most of FY15, LCS 2 returned to San Diego in February and has remained in port in a maintenance status for the majority of FY16, to include the conduct of a planned dry-docking selected restricted availability.

MCM Mission Package Activity

- In October 2015, the Navy delayed the IOT&E of the *Independence*-variant LCS equipped with the first increment of the MCM mission package pending the outcome of an independent program review, including an evaluation of potential alternatives to the RMS. The Navy chartered the review in response to an August 21, 2015, letter from Senators John McCain and Jack Reed, Chairman and Ranking Member of the Senate Armed Services Committee, expressing concerns about the readiness to enter operational testing given the significant reliability problems observed during a Technical Evaluation in 2015.
- In early 2016, following the completion of the independent review, the Navy:
  - Concluded that reliance on shore-based test metrics provided a false sense of RMMV maturity and contributed to the RMS progressing to sea-based test events prematurely.
  - Cancelled the RMS program and halted further RMMV procurement.
  - Announced its intention to field existing RMMVs following overhauls intended to mitigate high impact failure modes.
  - Indicated a desire to accelerate development of Knifefish UUV pre-planned product improvements, which are funded in the FY18-23 Knifefish budget.
  - Revealed initial plans (subsequently dashed by lack of funding for Knifefish improvements) to evaluate alternatives to the RMS, including an unmanned surface craft towing either the AN/AQS-20C or AN/AQS-24C minehunting sensor and an improved version of the Knifefish UUV already in development.
  - Abandoned plans to conduct operational testing of individual MCM mission package increments and delayed the start of LCS MCM mission package IOT&E until at least FY20.
  - Announced plans to delay IOT&E of the LCS-based AMCM systems (MH-60S with ALMDS and the MH-60S with AMNS) and declare an IOC for these systems in early FY17.
- In May 2016, DOT&E provided comments on the Navy's draft Capability Development Document for the Barracuda Mine Neutralization System. The Navy approved the Barracuda Mine Neutralization Capability Development Document in September 2016.
- In FY16, the Navy continued development of the COBRA Block I system, and conducted developmental testing of the system from a modified U.S. Army UH-1H "Huey" helicopter and MQ-8B airframes. The Navy expects to complete operational testing of the COBRA Block I system in 2017, including a demonstration of LCS integration and an assessment of potential cybersecurity vulnerabilities.
- The Navy continued development of UISS and plans to commence developmental testing in FY17. As part of the initial effort to identify two suitable test sites for future operational testing, the Navy employed a prototype system to characterize the magnetic properties of two environments in FY16. Since the results of these events indicate the two environments the Navy examined are not magnetically diverse, additional environmental characterization will be necessary to ensure that future operational testing spans a representative portion of the system's expected operating regime.
- Throughout 2016, the Navy continued to develop the mine-like Navy Instrumented Threat Target (NAVITTAR), which is a key resource for future developmental and operational testing of the UISS and a potential training asset for the fleet. Although the Navy is developing instrumented targets to imitate a variety of threat mines, the pace of NAVITTAR development and production

raises considerable doubts about whether both moored and bottom targets will be available in sufficient quantities to support the developmental and operational testing of UISS planned in FY17 and FY18. The Navy also employed early NAVITTARs to collect environmental characterization data, but observed multiple incidents in which an instrumented target failed to collect the expected data, raising additional doubts about the adequacy of this critical test resource.

- The Navy continued to develop pre-planned product improvements for the AN/AQS-20 sonar in FY16. The Navy's plans to commence realistic AN/AQS-20C developmental and operational testing are unsettled because of limited availability of two potential tow platforms; existing RMMVs are not reliable but the Navy does not expect to make the initial, limited-quantity USVs compatible with the AN/AQS-20C until late FY18. In testimony to the Senate Armed Services Committee in December, the Navy announced that two RMMVs will be groomed and one will be overhauled. These RMMVs will then be used to continue AN/AQS-20 sonar testing, conduct data collection, and support user evaluation until the first USV is available.
- During FY16, the Knifefish program focused on hardware qualification testing and limited at-sea contractor testing in preparation for future developmental and operational testing. The Knifefish contractor is fixing failures identified in contractor testing. Contingent on adequate program funding, the Navy expects to continue developmental testing (DT), followed by an operational assessment in FY17. The Navy plans to start Knifefish IOT&E in FY18.
- In 2016, the Navy reallocated funding intended to support near-term ALMDS pre-planned product improvement development. The Navy also reported that the improved system would not be available to the LCS MCM mission package until at least FY21, thus indicating it will not be available in time to support the planned LCS MCM mission package IOT&E (in FY20).
- In September 2016, the Navy announced that it plans to use fleet exercises to gather additional data to characterize previously unknown attributes of the AMCM systems it plans to IOC in FY17. For ALMDS, the Navy expects to characterize the system's probability of detection and classification as a function of mine spacing and water depth. For AMNS, the Navy expects to characterize performance of the system against buried mines.
- The Navy is considering various LCS MCM mission package configurations that could be optimized to support mine hunting or mine sweeping operations but it has not established a concept of operations for using one or more of these LCS MCM mission package configurations to support MCM missions.

SUW Mission Package Activity

- In March 2016, DOT&E published a partial assessment of the radar-equipped MQ-8B's performance based on the Navy's Quick Reaction Assessment (QRA) conducted in 2015. The Navy deployed the MQ-8B as part of the SUW mission package on LCS 4 during its brief 2016 deployment; however, the air vehicle has never been operationally tested in conjunction with the SUW mission package on any LCS, so its capabilities and limitations in realistic environments are largely unknown.
- In June 2016, DOT&E published an operational assessment of the MQ-8C based on the testing conducted in November 2015. This report evaluated the MQ-8C sensor and air vehicle performance, but did not include an evaluation of the MQ-8C's ability to contribute to LCS missions or its interoperability with LCS and the SUW mission package. Operational testing of the MQ-8C and the mission package is planned for FY18.
- The Navy began developmental testing of the Increment 3 SUW mission package, completing initial Longbow HELLFIRE missile firing events from a barge in December 2015 and August 2016. The Navy planned to conduct the first structural test firing from an LCS fitted with a Surface-to-Surface Mission Module (SSMM) in September 2016, but that test was postponed until FY17. The Navy hopes to conduct ship-based developmental testing in 2017 in anticipation of Increment 3 operational testing in early FY18 aboard a *Freedom*-variant LCS.

ASW Mission Package Activity

- The Navy did not conduct any at-sea testing of the ASW mission package in FY16. The Navy continued its efforts on a weight reduction program for the components of the mission package, including the handling system and support structures for the variable depth sonar and multifunction towed array. The Navy anticipates downselecting to a single vendor for the variable depth sonar in FY17 and beginning a test program soon thereafter.
- In September 2015, the Navy completed a formal study that identified capability gaps in currently available torpedo surrogates and presented an analysis of alternatives for specific investments to improve threat emulation capability. The Navy has since taken the following actions to address the identified capability gaps:
  - The Navy received approximately $1.0 Million through an FY16 Resource Enhancement Project (REP) proposal and is currently in development of a threat-representative high-speed quiet propulsion system.
  - The Navy submitted an FY17 REP proposal for $6.2 Million to develop a General Threat Torpedo (GTT) that will expand upon the propulsion system under development and provide representation of threat torpedoes in both acoustic performance and tactical logic.

Assessment

Program

- The Navy's original plans to field multiple increments of each mission package as systems mature have changed. The Navy now plans to field a single increment of the ASW mission package. The fourth increment of the SUW mission package is not funded and the Navy intends to complete the SUW mission package with the introduction of the SSMM in Increment 3. Plans for the MCM mission package are uncertain with the recent cancelation of the RMS program and the continued development of multiple other minehunting and neutralization systems.

- The Navy completed initial phases of operational testing in FY14 for the *Freedom* variant with an embarked Increment 2 SUW mission package, and in FY16 for the *Independence* variant with an embarked Increment 2 SUW mission package. The final phases of operational testing will not be completed until the full mission package capability is available. The Navy expects to complete those final phases of operational testing of the ASW and SUW Increment 3 mission packages in FY18.
- The Navy was successful in articulating adequate operational test designs in an update to the LCS TEMP for the SUW, ASW, live fire, and air defense systems. In addition, despite uncertainty in MCM mission package plans, the Navy was also able to develop a high-level strategy for future MCM testing. However, the TEMP does not yet include plans for developmental or integrated testing of these systems, which should be added before testing begins.

Seaframes

- DOT&E has now evaluated both seaframe variants to be not operationally suitable because many of their critical systems are unreliable, and their crews do not have adequate training, tools, and documentation to correct failures when they occur. No matter what mission equipment is loaded on either of the ship variants, the low reliability and availability of seaframe components, coupled with the small crew size, imposed significant constraints on mission capability. During this last year, problems with main engines, waterjets, communications, air defense systems, and cooling for the combat system occurred regularly and required test schedules to be revised or operations to be conducted with reduced capability (e.g., conducting MCM missions without operational air defense systems). These reliability problems are often exacerbated because, by design, the ship's force is not equipped to conduct extensive repairs; problems cannot be corrected quickly due to the need to obtain vendor support, particularly when several vendor home bases are at disparate overseas locations. The inability of the ship to be ready at all times to reach maximum speed, keep its main air defense system in operation, and to cool its computer servers are substantially detrimental to the ships' ability to defend themselves in time of war, much less conduct their assigned missions in a lengthy, sustained manner.
- The Navy has not conducted any of the planned live-fire air defense test events planned as part of the Enterprise Air Warfare Ship Self Defense TEMP or recently updated LCS TEMP. After multiple years of delays, the Navy had planned to conduct the first of those events on the self-defense test ship in FY16, but postponed the test indefinitely because of anticipated poor performance predicted by pre-test modeling and analysis of the planned test event scenario. Without these tests, an adequate assessment of the *Independence*-class probability of raid annihilation requirement is not possible. DOT&E expects that the *Independence* variant will have been in service nearly 10 years by the time that air defense testing is complete, which at the time of this report is not anticipated before FY20.
- The Navy has identified it is not satisfied with the *Freedom* variant's radar and RAM system for defense against ASCMs. The Navy plans to replace the RAM system with SeaRAM, which is the system installed on the *Independence* variant. The Navy does not plan to test the existing *Freedom*-variant air defense systems installed on LCS 1 through 15. DOT&E assesses this to present a high risk for deploying crews, given that many *Freedom*-variant ships will deploy between now and 2020 when backfits of the SeaRAM system on those hulls are scheduled to begin.
- Neither LCS variant has been operationally tested to evaluate its effectiveness against unmanned aerial vehicles and slow-flying aircraft. Although the Navy had planned to test the *Independence* variant's capability to defeat such threats in FY15, the testing was canceled in part due to range safety requirements that would have precluded operationally realistic testing. DOT&E concurred with this decision because proceeding with an unrealistic test would have been a needless waste of resources.
- In the report to Congress responding to the NDAA for FY16, DOT&E noted that the envisioned missions, use of unmanned vehicles, and operating environments have shifted relative to the original LCS vision. DOT&E concluded that the current plan to employ LCS as a forward-deployed combatant, where it might be involved in intense naval conflict, appears to be inconsistent with its inherently poor survivability in those same environments.
- The ability of LCS to perform the bulk of its intended missions (SUW, MCM, ASW) depends on the effectiveness of the mission packages. To date, the Navy has not yet demonstrated effective capability for the MCM, SUW, or ASW mission packages. The Increment 2 SUW mission package has demonstrated some modest ability to aid the ship in defending itself against small swarms of fast-inshore attack craft (though not against threat-representative numbers and tactics), and the ability to support maritime security operations.
- The intentionally small crew size has limited the mission capabilities, combat endurance, maintenance capacity, and recoverability of the ships. The core crew of *Independence* seaframes does not include sufficient watchstanders qualified to operate the seaframe combat system to maintain an alert posture for extended periods of time. During normal peacetime operations, the combat systems can be overseen by a single combat system manager (CSM), but in any elevated threat environment the manning plan calls for two CSMs to stand watch together to reduce overtasking. Since the ship's crew includes only three qualified CSMs,

the ship cannot maintain this alert posture for extended periods, such as might be required when transiting through contested areas, or escorting a high-value unit.
- In September 2016, the Navy released new plans to change the crewing structure. The Navy plans to phase out the 3-2-1 crewing construct and transition to a Blue/Gold model similar to the one used in crewing Ballistic Missile submarines. Originally, core crews and mission module crews were intended to move from hull to hull independently of one another; core crews will now merge with mission module crews and focus on a single warfare area – either SUW, MCM, or ASW. DOT&E does not yet have sufficient information to assess whether the new crewing model will solve the problems observed in the testing of both variants and whether ships will continue to be heavily dependent on Navy shore organizations for administrative and maintenance support.

• *Freedom* Variant Seaframe (LCS 1 and 3):
  - DOT&E's FY15 annual report as well as the comprehensive classified report issued in December 2015 described DOT&E's assessment of the *Freedom* variant. The Navy did not conduct any additional testing or perform any modifications to the seaframe in 2016 that would affect these assessments.

• *Independence* Variant Seaframe (LCS 2 and 4):
  - Although not all aspects of operational effectiveness and suitability could be examined during the 2015/16 operational test, that testing identified shortcomings in cybersecurity, air defense, surface self-defense, reliability, maintainability, and other operations, which are detailed in the DOT&E November 2016 classified report. DOT&E will issue an operational test report following the testing of the final increment of the SUW mission package to support acquisition decision making regarding the Full-Rate Production decision for the SUW mission package and other aspects of the LCS program.
  - **Air Defense.**
    ▪ In the Navy-conducted non-firing radar tracking events against subsonic ASCM drones, the Sea Giraffe radar provided LCS crews with only limited warning to defend itself against ASCMs in certain situations.
    ▪ In the Navy-conducted testing of the *Independence* variant's ES-3601 ESM system, the Navy used Learjet aircraft equipped with ASCM seeker simulators to represent the ASCM threats. The ES-3601 detected the presence of the ASCM seekers in most instances but did not reliably identify certain threats. Classified results are contained in DOT&E's operational test report of November 2016.
    ▪ In the developmental test events evaluating the ship's capability to detect, track, and engage so-called low slow flyers (LSFs) (unmanned aerial vehicles, slow-flying fixed-wing aircraft, and helicopters), the only sensor used to provide tracking information for engaging LSFs with the 57 mm gun was the SAFIRE electro-optical/infrared system. The test events demonstrated that SAFIRE was unable to provide reliable tracking information against some targets. Furthermore, the safety standoff requirements on Navy test ranges were so severe that they precluded meaningful live-fire gun engagements against these targets. Because of these problems and constraints, the program decided to cancel all subsequent live-fire events, including those scheduled for operational testing, conceding that the *Independence* variant is unlikely to be consistently successful when engaging some LSFs until future upgrades of SAFIRE can be implemented. Future testing against LSFs will not be possible until the Navy finds a solution to the severe safety constraints that preclude engaging realistic targets.
    ▪ Although the Navy has postponed indefinitely its plans to conduct live-fire testing of the LCS air defense systems, the Navy has conducted some initial testing of the SeaRAM system, as it is employed aboard Arleigh Burke destroyers. In the Navy-conducted live-fire event aboard the self-defense test ship, the SeaRAM system was successful at defeating a raid of two GQM-163 supersonic targets. Although a stressing event, these targets were not representative of the threats they were attempting to emulate. The Navy does not currently have an aerial target that is capable of emulating some modern ASCM threats. During this test, SeaRAM employed the RAM Block 2 missile, which is different than the current LCS configuration that employs the RAM Block 1A missile. However, if the Navy decides to deploy LCSs with the Block 2 missile, then this test and others planned are germane to an LCS evaluation, however incomplete. DOT&E and the Navy continue to conduct test planning to optimize the available resources and ensure that LCS's air defense testing reflects the capabilities of deploying LCSs.
  - **Surface Self-Defense.** The Navy conducted seven test events (four integrated test events and three dedicated operational test events), each consisting of a single attacking small boat. LCS was required to defeat the boat before it reached a prescribed keep-out range. LCS failed to defeat the small boats in two of the events.
    ▪ The 57 mm gun demonstrated inconsistent performance even in benign conditions, which raises doubts about the ship's ability to defend itself without the SUW mission package installed. The inaccuracy of the targeting systems, the difficulty in establishing a track on the target, and the requirement to hit the target directly when using the point-detonation fuze combine to severely impair effective employment of the gun, and limit effective performance to dangerously short ranges. The Navy has not conducted any testing to determine how well the ship will perform when faced with an attack in a realistic cluttered maritime environment including both neutral

and hostile craft; the Navy has also not conducted operational testing to determine how well the ship (without the SUW mission package) will perform against multiple attacking boats. Nevertheless, given the performance observed during operational testing, the combination of faster threats, multiple threats, threats with longer-range standoff weapons, cluttered sea traffic, or poor visibility is likely to make it difficult for LCS (without the SUW mission package) to defend itself.

- The ship's electro-optical/infrared camera, SAFIRE, is the primary sensor for targeting the 57 mm gun. The system suffers from a number of shortcomings that contribute to inconsistent tracking performance against surface and air targets, including a cumbersome human-systems interface, poor auto-tracker performance, and long intervals between laser range finder returns. These problems likely contributed to the poor accuracy of the 57 mm gun observed during live-fire events, though the root cause(s) of the gun's inaccuracy has not been determined definitively.
- Both of the failures of the surface self-defense test events were caused by MK 110 57 mm gun malfunctions. During the first presentation, the Proximity Fuze Programmer failed, causing all rounds to be fired in the default proximity mode, which then exploded in midair. The crew was unable to repair the failure and continued to fire the gun during the event until the target broached the minimum safety range. Technicians subsequently repaired the gun on July 7, 2015. The second failed event occurred on July 18 when the 57 mm gun jammed during the event. With the assistance of a civilian gun system technician, the crew downloaded the remaining ammunition, cleared the jam, and restored the gun to "single-sided" operation in about 4 hours by consolidating good components. Until repaired on August 7, 2015, the gun was limited to firing 60 rounds, rather than its normal 120, before reloading.
- On two occasions, the shock caused by firing the 57 mm gun unseated network cards, disabling the steering controls on the bridge and forcing the crew to steer the ship from an alternate location. On another occasion, gunfire shook network cables loose, disabling the 57 mm gun. Although the ship was able to recover from these failures within a few minutes and continue the engagement, these types of interruptions have the potential to prolong the ship's exposure to an advancing threat, as was observed during testing.
- In the most recent of the seven live fire test events the Navy conducted against a single-boat target, the crew employed the 57 mm differently than it had in previous live-fire events, and defeated the attacking boat with less ammunition and at a slightly longer range than in previous events. One event does not provide conclusive evidence that the ship can be effective in these scenarios, and such performance was never observed during the swarm-defense test events. Nevertheless, these results are encouraging and suggest that the Navy should examine tactics and alternative gun employment modes, including different projectile fuze settings, as a means to enhance LCS's currently limited capabilities.

- **Missions of State.** LCS 4 completed six mock Missions of State during the 2015 test period requiring the launch and recovery of two 11-meter rigid hull inflatable boats (RHIBs). Although the ship demonstrated the capability to meet Navy requirements for the timely launch of two 11-meter RHIBs to support effective Visit, Board, Search, and Seizure operations in Sea State 2 and below, the time needed to recover the boats aboard ship often exceeded the Navy requirement because of problems with the surface tow cradle and the twin-boom extensible crane (TBEC). Testing revealed operational deficiencies and safety concerns. Observers reported that flaws in the design of the surface tow cradle used in conjunction with the watercraft launch, handling, and recovery system and other problems limit safe launch, internal movement, and recovery of boats to Sea State 2 and below. The cumbersome multi-step boat launch/recovery process has several "single points of failure" – including the surface tow cradle, TBEC, the Mobicon straddle carrier, and a forklift – that increase the likelihood of delays and the possibility of mission failure. The failure of any of these components can halt boat operations and could leave a boat stranded at sea, which happened once during operational testing.
- **Endurance and Speed.** LCS 4 met its transit range requirement, demonstrating a fuel usage rate that enables it to travel more than 4,200 miles at 14 knots if called upon to do so (threshold 3,500 miles). LCS 4 failed its sprint speed requirement of 40 knots, demonstrating a maximum sustained speed of only 37.9 knots in calm waters. It fell just short of its sprint range requirement (1,000 miles at maximum speed), demonstrating fuel burn rates at maximum speed that would enable it to travel 947 miles. LCS 4 has long-standing problems with her ride control system hardware, including interceptors, fins, and T-Max rudders, that affect the ship's maneuverability at high speeds. The ship also had reported recurring problems with frequent clogging of the gas turbine engine fuel oil conditioning module pre-filters and coalescers, and found it difficult to maintain high speed for prolonged periods. The crew found it necessary to station extra operators in the machinery room (normally an unmanned space) to change fuel filters and manually control the fuel oil heaters to keep the gas turbine engines in operation during these high-speed runs.
- **Cybersecurity.** In early 2016, the Navy made substantial changes to the LCS 4's networks, calling

the effort "information assurance (IA) remediation," to correct many of the deficiencies in network security on the baseline *Independence* variant's total ship computing environment. Previous testing on LCS 2 in 2015 revealed several deficiencies in network protection such as the lack of proper settings and access controls, poor network segmentation, and lack of intrusion detection capabilities. The Navy designed and implemented the IA remediation program to mitigate or eliminate such vulnerabilities and was successful in eliminating some of the deficiencies that placed the ship at risk from cyber-attacks conducted by nascent (relatively inexperienced) attackers.

- DOT&E found that the Navy's testing, which included a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment in 2016 on LCS 4, was inadequate to fully assess the LCS 4's survivability against cyber attacks originating outside of the ship's networks (an outsider threat). The testing was adequate to determine that some deficiencies remain when attacks occur from an insider threat, however, it was not adequate to determine the full extent of the ship's cybersecurity vulnerability or the mission effects of realistic cyber-attacks. Because of the imminent deployment of LCS 4, the Navy did not allow cybersecurity testers to make changes to the configuration of network components, as a cyber aggressor would almost certainly attempt to do to gain a foothold on the system. Testing was also impeded by electrical work, test site disruptions, and frequent network configuration changes because the test was conducted during a maintenance period. Because of these changes and the installation of systems (including the Harpoon missile and MQ-8B Fire Scout and its control system) after the test completed, DOT&E is uncertain whether an operationally representative configuration of the system was tested. Lack of physical access to many systems imposed by test artificialities, restrictions on the test team, and inadequate test preparation also limited the conduct of the test. The duration of Adversarial Assessment was reduced to less than half the original plan because of the delays experienced during the CVPA. Finally, DOT&E found that the Navy Operational Test Agency's threat emulation used for this test was lacking and did not meet the standards necessary for a robust cybersecurity examination. In July 2016, DOT&E issued guidance on cybersecurity test methods to all of the Service operational test agencies, in part due to the inadequacies in threat emulation observed in the LCS cybersecurity testing.
- Although the Navy's IA remediation corrected some of the most severe deficiencies known prior to the test period, the testing revealed that several problems still remain which will degrade the operational effectiveness of *Independence*-variant seaframes until the problems are corrected. The Navy reported that the second phase of IA remediation intended to correct additional network deficiencies has been installed on all follow on ships; however, DOT&E is unaware of the plans to test these changes on future ships, or whether these changes will correct the problems observed during the LCS 4 test.

- **Operational Suitability.** The *Independence* variant (with or without a mission package) is not suitable for SUW missions or MCM missions, and will remain that way until the Navy can reduce the failure rates of mission-essential equipment and correct the deficiencies that require workarounds and unsustainable manning. Unless corrected, the critical operational suitability problems highlighted below will continue to prevent the ship and mission packages from being operationally effective.
- **<u>LCS 2 Reliability and Availability</u>.** Although not tested in 2016, DOT&E's June 2016 early fielding report on the LCS 2 equipped with the MCM mission package delineated the suitability of the *Independence* variant. The type and severity of the failures observed on LCS 4 were also observed on LCS 2 during the 2015 Technical Evaluation period for the MCM mission package, suggesting that the reliability and availability problems observed are inherent to the *Independence*-variant seaframe, rather than isolated to one hull. The MCM mission package places different and greater demands on seaframe equipment than does the SUW mission package. The frequency of seaframe failures observed on the LCS 2 seaframe with the MCM mission package was greater than that observed on LCS 4 with the SUW mission package; implying the frequency of *Independence* variant seaframe failures and associated availability are likely mission package dependent (i.e., mission dependent). The following are the most significant seaframe equipment problems observed during the 2015 Technical Evaluation period.
  - Recurring failures of the main propulsion diesel engines and their associated water jet assemblies hindered test operations throughout the test period. LCS 2 was unable to launch and recover RMMVs on 15 days because of four separate propulsion equipment failures involving diesel engines, water jets, and associated hydraulic systems and piping. These failures would also have limited the ship's capability to use speed and maneuver to defend itself against small boat threats.
  - LCS 2 experienced multiple air conditioning equipment failures and was unable to supply enough cooling to support the ship's electronics on several occasions. One or more of the ship's three chilled water units was either inoperative or operating at reduced capacity for 159 days (90 percent of the period).

- LCS 2 experienced failures of critical systems such as the SeaRAM air defense system (four failures and a total downtime of 120 days), the ship's 57 mm gun (inoperative for 114 days), the SAFIRE electro-optical/infrared system (inoperative for 25 days), and the Sea Giraffe radar (multiple short outages) that were not repaired immediately because they did not preclude continuation of MCM testing in an environment devoid of air and surface threats. These failures would not have been ignored in a contested location; and many of these failures left the ship defenseless against certain threats for days at a time. Had these failures occurred in theater, the repair efforts would have affected MCM operations, likely forcing the ship off-station to effect repairs and/or embark technicians since the crew does not have the requisite training, parts, or documentation to effect repairs themselves.
- Similar to LCS 4, LCS 2 experienced several Ship Service Diesel Generator failures during the period, but was never without at least two of four generators operable (sufficient to power all combat loads, but which leaves the ship with no redundancy in the event of another failure).
- A Mobicon straddle carrier failure left the ship unable to conduct waterborne MCM operations for a period of 4 days until a technician could travel from Australia to diagnose the problem and make needed adjustments. This episode demonstrated the crew's paucity of documentation, training, and diagnostic equipment.
- Failure of a power conversion unit that supplied 400-Hertz power to the mission bay deprived the ship of MCM mission capability for 20 days while the ship was in port undergoing repairs. The ship also lost the capability to supply 400-Hertz power to the aircraft hangar, where it is needed to conduct pre-mission checks on the MH-60S and AMCM systems. The Navy never determined the cause of the near-simultaneous failures of the two power conversion units, although technicians considered them related.

- **LCS 4 Reliability and Availability.** The mission-essential equipment for conducting SUW on LCS 4 had poor reliability, with a failure that caused a partial loss of capability approximately every day and a complete loss of mission capability every 11 days on average. Based on these failure rates, LCS has a near-zero chance of completing a 14-day mission (the length of time LCS can operate before resupply of food is required) or a 30-day mission (the length of time prescribed by Navy requirements documents) without experiencing an operational mission failure. When averaged over time, and accounting for both planned and unplanned maintenance downtimes, the ship was fully mission capable for SUW missions 24 percent of the 2015 test period, and was fully or partially mission capable 66 percent of the time. The following are the most significant seaframe equipment problems observed during the 2015-2016 developmental and operational test periods.

- LCS 4 suffered numerous failures of its propulsion systems, including the diesel engines, gas turbines, and steerable waterjets. The most debilitating problems occurred during the first developmental testing period in May and June 2015, when a combination of failures left the ship with only one working engine for 19 days. Following the July 2015 in-port maintenance period, the reliability of the propulsion systems improved, but single engines and waterjets continued to fail, and LCS spent 40 days of the 136-day test period with one or more engines inoperative or degraded. During the 2016 test periods, observers continued to report failures to the diesel engines and gas turbines that limited the ship's speed.
- LCS 4 was seldom able to keep all three air conditioning units fully operational. In one case, the systems were unable to supply enough cooling to support the ship's electronics for a 2-week period. The Navy recognized that the commercial off-the-shelf chilled-water air conditioning systems installed in LCS 2 and LCS 4 had serious reliability problems and, working with the shipbuilder, sourced the air conditioning systems on LCS 6 and follow-on *Independence* seaframes from a different manufacturer. Since the LCS program has not replaced the air conditioning systems on LCS 2 and LCS 4, those systems are still exhibiting severe reliability problems.
- LCS 4 experienced several Ship Service Diesel Generator failures during the periods of observation, but was never without at least two of four generators operable (sufficient to power all combat loads, but which leaves the ship with no redundancy in the event of another failure). Problems with electrical switchboards added to the difficulties, as certain combinations of diesel generators would not share load, reducing the redundancy in the system. Observers recorded four load sheds, which automatically severed power to non-essential systems, and in one case, caused key combat systems to shut down.
- During the 2015 test events, LCS 4 experienced numerous instances in which the flow of navigation data (heading, pitch, and roll) to the combat system was disrupted for short periods, which disabled the Sea Giraffe radar and the 57 mm gun and degraded SeaRAM's performance. The worst recorded instance occurred during the September 2015 live fire gun event when the flow of navigation data was interrupted 34 times, leading to a loss of all tracking information and the inability to fire the 57 mm gun

for nearly 30 minutes. These outages significantly affected the crew's ability to defeat targets and contributed to the ship's failure to defeat all targets before they entered the keep-out zone. The problem defied early troubleshooting efforts and persisted into early 2016; however, observers did not report any navigation data outages after testing resumed in 2016, indicating that the Navy may have corrected the problem during installation of the IA remediation upgrades and other system changes. The Navy reported that the first instances of navigation data outages observed in 2015 were attributable to a cabling failure; and that the root cause of the failure was determined and corrected permanently. The Navy determined that the navigation data outages observed in 2016 were caused by the IA upgrade that had been recently installed in LCS 4 in early 2016; and the outages were remedied by reverting the network core switches back to the pre-IA upgrade routing protocol.

- The *Independence* variant's primary air defense system, SeaRAM, suffered from poor reliability and availability before, during, and after operational testing aboard LCS 4. Failures caused seven long periods of downtime (greater than 48 hours) between May 16, 2015, and June 18, 2016. Each repair required the delivery of replacement components that were not stocked aboard the ship, and most required assistance from shore-based subject matter experts. These failures left the ship defenseless against ASCMs, and would likely have forced it to return to port for repairs if it had been operating in an ASCM threat area. In addition, the SeaRAM aboard LCS 4 had five short (less than 5 minute) outages during live and simulated engagements against aerial targets, each of which might have resulted in an inbound ASCM hitting the ship. The SeaRAM aboard LCS 2 has also suffered from several long-lived failures.
- The ship's ride control system, used for high-speed maneuvering, did not appear to be fully functional at any time during developmental or operational testing in FY15 and FY16.

SUW Mission Package

- While equipped with the Increment 2 SUW mission package, LCS 4 participated in three engagements with small swarms of fast-inshore attack craft (small boats). LCS 4 failed the Navy's reduced requirement for interim SUW capability, failing to defeat each of the small boats before one penetrated the prescribed keep-out zone in two of the three events. Although LCS eventually destroyed or disabled all of the attacking boats in these events, the operational test results suggest that the Increment 2 SUW mission package provides the crew with a moderately enhanced self-defense capability (relative to the capability of the 57 mm gun alone) but not an effective offensive capability. In all three events, the ship expended an inefficiently large quantity of ammunition from the 57 mm gun and the two mission package 30 mm guns, while contending with azimuth elevation inhibits that disrupted or prevented firing on the targets. In one event, frequent network communication faults disrupted the flow of navigation information to the gun systems further hindering the crew's efforts to defeat the attacking boats. SAFIRE is a likely contributor to the observed 57 mm gun performance and large ammunition expenditure during surface engagements, and its cumbersome user interface contributed to the workload of already-overtasked watchstanders. LCS 4's failure to defeat this relatively modest threat routinely under test conditions raises questions about its ability to deal with more realistic threats certain to be present in theater, and suggests that LCS will be unsuccessful operating as an escort (a traditional frigate role) to other Navy ships. Additional details about the LCS gun performance and the factors and tactics that contribute to the ship's effectiveness are discussed in DOT&E's November 2016 classified report.
- The Navy has begun work on developing and testing the SSMM, the core component of the Increment 3 mission package. Operational testing in 2015 and 2016 revealed that the ship's radar, the only sensor available to provide initial targeting information to the Longbow HELLFIRE missiles employed from the SSMM, demonstrated performance limitations that might hinder its ability to support missile employment against small boat swarms. The Navy intends to conduct additional developmental testing to better understand these limitations; and the results of these tests will be used to inform future decisions by the Navy to modify missile targeting algorithms and tactics, as needed to overcome the limitations. The Navy plans to demonstrate the ability to meet the original LCS requirements for SUW swarm defense during operational testing of the Increment 3 mission package in FY18.

MCM Mission Package

- DOT&E concluded in a June 2016 early fielding report, based exclusively on the testing conducted before 2016, that an LCS employing the current MCM mission package would not be operationally effective or operationally suitable if called upon to conduct MCM missions in combat. The primary reasons for this conclusions are:
  - Critical MCM systems are not reliable.
  - The ship is not reliable.
  - Vulnerabilities of the RMMV to mines and its high rate of failures do not support sustained operations in potentially mined waters.
  - RMMV operational communications ranges are limited.
  - Minehunting capabilities are limited in other-than-benign environmental conditions.
  - The fleet is not equipped to maintain the ship or the MCM systems.
  - The AMNS cannot neutralize most of the mines in the Navy's threat scenarios.
- In the same early fielding report, DOT&E concluded that the current versions of the individual systems that

comprise the current MCM mission package, specifically the RMS and the MH-60S AMCM helicopter equipped with ALMDS or AMNS, would not be operationally effective or operationally suitable if called upon to conduct MCM missions in combat.

- Although the Navy has implemented some corrective actions to mitigate the problems observed in earlier testing, the substantive unclassified details of DOT&E's assessment are unchanged from the FY15 edition of this report. DOT&E's classified June 2016 early fielding report provides additional detail.
- Developmental MCM Systems. The Navy is continuing to develop the COBRA Block I, Knifefish, and UISS programs and has not yet conducted operational testing of these systems. However, early developmental testing or contractor testing of COBRA Block I and Knifefish have revealed problems that, if not corrected, could adversely affect the operational effectiveness or suitability of these systems, in operational testing planned in FY17 or FY18, and subsequently the future MCM mission package. In addition to the problems observed in early testing of developmental systems, DOT&E used lessons learned from earlier testing of the RMS to identify problems that are likely to affect the upcoming phases of Knifefish and UISS operational testing.
  - During developmental testing of COBRA Block I in early FY16, test data revealed that the system's probability of detection is low against small mines and mines emplaced in some environmental conditions. Thus, without improvements, the capability of the current system will likely be limited in some operationally realistic threat scenarios. Operational testing, planned for 2017, will characterize the COBRA Block I capability against a broader range of operationally realistic conditions.
  - For the Knifefish UUV program, the Navy's developmental efforts are currently focused on system design and have not yet tested Knifefish integration with either LCS seaframe variant. The Navy needs to test battery charging, off-board communications, maintainability, launch and handling equipment and procedures, and the ability of the crew to recover the vehicle reliably while employing the proposed grappling hook capture device to support Knifefish operations on both LCS variants. In addition, it is not yet known how Knifefish operations will be affected by concurrent LCS MCM activities, making operationally realistic testing of the Knifefish UUV in the combined MCM mission package essential.
  - The Knifefish vehicle's low frequency broadband sonar is designed to detect bottom, moored, and buried mines. After early contractor testing revealed that sonar transmitter elements were failing prematurely, the Naval Research Laboratory recommended operating the elements at a significantly lower voltage to extend their operational life. While this change will likely improve the sonar's reliability, the reduction of the sonar's transmitting power will also likely reduce the range at which the sonar can detect objects. Although the operational implications of these changes are not yet known, the actions taken to mitigate reliability problems could negatively affect the assessment of operational effectiveness in the upcoming operational assessment.
  - Knifefish contractor testing in October uncovered a UUV structural failure mode during launch in which the vehicle broke in half during launch from a test ship. The contractor analyzed the failure and suspects it was caused by a combination of factors including the wave height encountered during launch, the vehicle position on the launch ramp, and the launch ramp geometry. The contractor is considering options to address this failure mode such as redesigning the launch ramp and restricting launches to lower sea states.
  - The UISS contractor delivered the first engineering development unit only recently and has not yet conducted testing of a production representative system. The Navy will need to consider integration challenges that include off-board communications, maintainability, launch and handling equipment and procedures, and the ability of the crew to recover the system safely and reliably. Although the Navy plans to characterize UISS performance in dedicated minesweeping scenarios during the initial phases of LCS-based testing, operationally realistic testing of the system in the combined MCM mission package is also essential.
  - Currently, LCS sailors do not possess an organic, in-situ means to measure environmental characteristics that are important to plan UISS minesweeping missions. Although the Navy is working on a solution that it hopes to make available by 2020, the lack of this capability may affect the LCS crew's ability to employ UISS effectively in upcoming operational testing that will characterize minesweeping performance over the range of conditions expected in potential threat scenarios.
- Current Navy plans for developing, integrating, and testing mine hunting and mine sweeping systems in the LCS MCM mission package are not adequately funded to mature the MCM capabilities to meet mission requirements.

ASW Mission Package

- The current threat torpedo surrogates have significant limitations in their ability to represent threat torpedoes. As such, operational assessment of each LCS variant with ASW mission package using these test articles will not fully characterize the ship's capability to defeat incoming threat torpedoes. The proposed development of a General Threat Torpedo (GTT) addresses many of DOT&E's concerns; however, the GTT's capability to support realistic operational testing depends on future Navy decisions to procure a sufficient quantity of GTTs.

LFT&E

- Neither LCS variant is expected to be survivable in high intensity combat because the requirements accept the risk of abandoning the ship under circumstances that would not require such an action on other surface combatants. Although the ships incorporate capabilities to reduce their susceptibility to attack, previous testing of analogous capabilities in other ship classes demonstrates it cannot be assumed LCS will not be hit in high-intensity combat. As designed, the LCS lacks the redundancy and the vertical and longitudinal separation of vital equipment found in other combatants. Such features are required to reduce the likelihood that a single hit will result in loss of propulsion, combat capability, and the ability to control damage and restore system operation.
- LCS does not have the survivability features commensurate with those inherent in the USS *Oliver Hazard Perry*-class Guided Missile Frigate (FFG 7) it is intended to replace. The FFG 7 design proved to retain critical mission capability and continue fighting after receiving a significant hit.
- The LCS 4 Total Ship Survivability Trial (TSST) exposed weaknesses in the *Independence*-variant design.
  - While the auxiliary bow thruster provided a limited means to recover propulsion, much of the ship's mission capability would have been lost because of the primary weapon damage or the ensuing fire and flooding.
  - Damage to chilled water system piping caused an unrecoverable loss of several vital systems because of equipment overheating. The chilled water system's lack of cut-off valves does not allow for isolation of damaged sections.
  - There is a lack of sufficient separation between the two damage control repair stations (DCRS). The Mission Bay Fire scenario resulted in the loss of both DCRS (one from the primary weapon effects and the second due to the spread of smoke as a result of the proximity to the fire boundary). The rescue and assistance locker located in the Helicopter Hangar is not outfitted with DCRS equipment exacerbating the damage control capability shortfalls.
  - Installed damage control systems, such as Aqueous Film Forming Foam (AFFF) and Main Drainage, are designed with motor-operated valves co-located in the compartments that the systems are supposed to protect. As a result, the crew could not access these valves to reconfigure the damaged systems when remote operation was compromised by loss of power or data.
- The Navy conducted a reduced severity shock trial on USS *Jackson* (LCS 6), executing three shots of increasing severity, ending at 50 percent of the maximum design level. The Navy decided not to test up to the standard 2/3 design level due to concerns the ship would suffer a large amount of damage to non-shock hardened mission-critical equipment.
- In addition to reducing the shot severity, the Navy took several protective measures to reduce the risk of equipment damage and personnel injury to include:
  - Removed some equipment before the trial or between shots, such as the Tactical Common Data Link antenna and racks, the navigational radar, and the 57 mm gun.
  - Replaced some rigid pipes with flexible connections.
  - Replaced some existing bolts with higher strength material.
  - Added cable slack in some locations.
  - Rerouted some ducts and pipes and modified ship structure to increase shock excursion space around equipment.
  - Strengthened some bulkheads where heavy equipment was attached.
  - Repaired missing and undersized foundation welds.
  - Tied life rafts to the ship to make sure they did not self-deploy during the shots.
- A preliminary assessment of the LCS 6 shock trial demonstrated that:
  - The Navy assumptions regarding the performance of non-hardened when exposed to underwater shock are overly conservative. The Navy assumed that these components and systems would become inoperable while the shock trial demonstrated most non-hardened components and systems remained operable or were restored to a limited or full capability prior to the ship's return to port on each shot.
  - The ship maintained electrical power generation through all three shots, to include the Non-Vital Ship Service Diesel Generators.
  - The SeaRAM system remained operable through all three shots.
  - The main gun survived shot one, but the Navy removed it for the later shots, conceding that severe damage was likely. The actual gun survivability/firing capability at higher shock severities cannot be assessed.
  - The auxiliary propulsion bow thruster remained operable through all three events.
  - The trimaran ship design displayed unique structural behaviors not seen in mono-hull ships. The attenuation of the shock loading above the keel invalidated the Navy approach of using a target keel velocity as the metric to determine shot shock severity and confidence in the pertinent M&S tools to capture the shock trial phenomena. Despite achieving a target keel velocity, the majority of the LCS 6 deck mounted equipment did not experience the shock severity intended by the Navy.
- Based on the LCS 6 shock trial lessons learned, the Navy conducted a shock trial aboard USS *Milwaukee* (LCS 5) from August 29 through September 23, 2016, starting the trial at more traditional severity levels. However, the Navy stopped the LCS 5 trial after the second shot, thereby not executing the planned third shot due to concerns with the shock environment, personnel, and equipment. The Navy

did not view the third LCS 5 shock event as worthwhile because of concerns that shocking the ship at the increased level would significantly damage substantial amounts of non-mission critical equipment, as well as significantly damage a limited amount of hardened, mission critical equipment, thereby necessitating costly and lengthy repairs.
- The electrical distribution system remained operable or was restored to a limited or full capability prior to the ship's return to port after each shot.
- Most non-hardened components and systems, including the RAM air defense system, remained operable or were restored to a limited or full capability prior to the ship's return to port after each shot.
- By not executing the 2/3 level shot, the Navy could not validate the overly conservative assumptions made for the underwater threat shot in the LCS 3 TSST.
- DOT&E will release a more comprehensive classified report in 2017 upon complete analysis of the trial data.

Recommendations

- Status of Previous FY15 Recommendations.
  - With respect to the MCM mission package and the cancellation of the RMS program, the Navy appears to have accepted the recommendation to shift to a performance-based test schedule rather than continuing a schedule-driven program. The LCS program needs ample time and resources to correct the numerous serious problems with the MCM mission package.
  - The Navy did not accept DOT&E's recommendation to obtain the intellectual property rights needed to develop high-fidelity digital models of the AN/SPS-75 (TRS-3D) and AN/SPS-77 (Sea Giraffe) radars for the Probability of Raid Annihilation Test Bed (a model used to evaluate the effectiveness of the LCS's air defenses). Although the Navy did respond to DOT&E's August 2015 memorandum, it appears that testing of the *Freedom*-variant's current configuration of air defense systems will be eliminated entirely, as LCS 17 and follow-on *Freedom* seaframes will be equipped with SeaRAM. This will leave the air defense capabilities of LCS 1 through 15 untested until the Navy backfits SeaRAM, which is not scheduled to begin until 2020.
  - The Navy has not yet accepted or addressed DOT&E's recommendation to improve the shock resistance of mission-critical electronics in the *Independence*-variant LCS. Until this problem is addressed, LCS is likely to experience a disruption in operations during 57 mm gun engagements and other shock-inducing activities/events.
  - The Navy has not yet formally addressed DOT&E's recommendation to work with the vendor to develop changes and improvements to SAFIRE, which are needed to improve the human-machine interface, reduce the time required to develop a new track, improve tracking, and correct other performance issues noted in FY15 testing. DOT&E reiterates this recommendation and suggests that the Navy also consider replacing the SAFIRE system with a more capable targeting system – one that is more user friendly and enables more accurate and effective gunfire for both air defense and SUW missions.
  - The Navy has begun to correct the causes of *Independence*-variant seaframe problems that disrupted gunnery engagements and other operations, however, several problems still remain that will preclude effective gun employment. The debilitating problem of the intermittent loss of navigation data appears to have been corrected; however, the Navy has not yet corrected the 30 mm gun azimuth-elevation inhibits, and the 57 mm gun's azimuth-dependent range errors. Azimuth-elevation inhibit errors or gun turret-drive errors occur intermittently and are of short durations, and prevent the gunner from firing during an engagement. During testing these errors frequently interrupted engagements at key moments. The Navy developed tactics, techniques and procedures that are now in use to mitigate the problem. The Navy is investigating the root cause of this disruptive error.
  - Despite the cancellation of the RMMV program, DOT&E's recommendation to re-engineer the communications system remains germane, as there is still a need for reliable line-of-sight and over-the-horizon communications between LCS and off-board vehicles. DOT&E recommends continued work to ensure the components of the MCM mission package can communicate reliability and operate over-the-horizon to enable LCS to have an effective MCM capability.
  - The Navy has not yet addressed DOT&E's recommendation to devise a safe method to realistically test the ships' ability to counter LSF threats. The Navy should coordinate with test range authorities to examine the feasibility of reducing the safety standoff restrictions; without changes, no meaningful test of LCS's capability against these threats can be conducted.
  - The Navy's recent change to the LCS concept of employment, which changes the crewing structure, training, and operational deployment of the class partially addresses DOT&E's recommendation to provide LCS crews with better training, technical documentation, test equipment, and tools, along with additional spares to improve the crews' self-sufficiency. It is not yet clear whether these changes will fully address the recommendation and will eliminate the maintenance problems DOT&E has articulated in multiple test reports.
  - The Navy and LCS program are improving their organic expertise with LCS systems; however, the Navy continues to maintain an outsized reliance on equipment vendors and overseas contractors, especially for the maintenance and repair of some critical mission equipment. DOT&E continues to recommend reducing this reliance on outside vendors to ensure crews and the Navy's in-service engineering agent can fully support LCS repair and maintenance activities.
  - As DOT&E recommended, the Navy is investigating options for re-engineering the recovery of watercraft;

however, no solutions have been found to correct the problems with RMMV recovery nor has the Navy demonstrated the ability to recover other vehicles like the Knifefish UUV.
  - The Navy has not made progress on developing tactics to mitigate system vulnerabilities to mines, mine collision, and entanglement hazards, and other surface and underwater hazards.
- FY16 Recommendations. Since December 2015, DOT&E issued three operational test reports for the LCS program, each of which contained multiple recommendations for the Navy's consideration that focus on the improvements needed to achieve operational effectiveness, suitability, and survivability, and to improve future testing. A selection of these recommendations is provided below.

Cybersecurity

1. After implementing changes to correct the deficiencies found in the LCS 4 cybersecurity test, conduct a full cybersecurity test, including a Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment. This testing should be conducted on a ship that has received the second phase of IA remediation and should examine the Increment 3 SUW mission package configuration. Future tests should include a range of malicious activities from stealthy to noisy to gain data needed to characterize the ship's detect and react capabilities and should not be conducted during a ship maintenance period (since this contributed to the inadequacy of the LCS 4 test events).
2. Ensure that vulnerabilities identified on one ship are remedied on all ships.
3. Schedule and conduct a comprehensive cybersecurity assessment of the MH-60S helicopter with ALMDS and with AMNS.
4. Expand future cybersecurity testing to include custom malware for system-specific operating systems and an examination of supervisory control and data acquisition systems and programmable logic controllers. Provide a stable ship configuration that accurately reflects the intended deployment configuration and allows for temporary changes to enable testers to examine mission-critical systems and evaluate the mission effects of cyber-attacks.

Seaframes

5. Develop a plan for integration of the MCM mission package with the *Freedom*-variant seaframe, including launch and recovery of MCM watercraft, and schedule early developmental testing to identify implementation challenges.
6. Improve reliability of mission systems and seaframe support systems to reduce logistics support requirements, crew workload, and unplanned downtime during MCM operations.
7. Improve the performance of the 57 mm gun system to increase the effective range and simplify targeting to enable faster and more lethal performance over a broader engagement range.
8. Improve the air-search radar on both seaframes to support earlier detections of ASCMs and tactical aircraft in both clear and jammed environments. Early detection increases the likelihood of survival against attack.
9. Increase the number of qualified Combat Systems Managers (CSMs) on the *Independence*-variant to provide additional operators for the seaframe sensors and guns.
10. Improve the reliability of the engineering systems, including diesel and gas turbine engines, steerable water jets, ride-control systems, and air conditioning equipment.
11. Determine the root cause of the *Independence* variant's fuel oil service system problems that occur during high-speed operations that made it necessary to station additional operators in the machinery room to replace Fuel Oil Conditioning Module pre-filters and control the fuel oil heaters manually.
12. Adequately fund the Air Warfare Ship Self-Defense Enterprise so that adequate testing of the LCS air defense systems can occur.
13. Improve the reliability and availability of SeaRAM.
14. Implement the equipment shock hardening measures employed on LCS 5 and 6 during the shock trial on all ships and survivability improvement findings/recommendations developed as a result of the two shock trial series.
15. Implement the survivability improvement recommendations developed by the LCS 4 TSST team. Most importantly, redesign the *Independence* variant's chilled water system to enable isolation of damaged sections.
16. Reevaluate LCS susceptibility to influence mines by conducting at-sea trials with the Advanced Mine Simulation System.

SUW Mission Package

17. Consider developing multi-ship tactics or build additional capability into future mission packages to enable LCSs, operating in surface action groups, to more effectively counter small-boat swarms that are more threat-representative.
18. Improve the 30 mm gun system's accuracy and expand the guns' effective range so that crews are not limited to a narrow region of success. Without improvements, LCS crews are unlikely to be successful against realistically sized small-boat swarms.

MCM Mission Package

19. Limit procurement of ALMDS, AMNS, and AN/AQS-20A systems, which have significant operational performance limitations that negatively affect LCS MCM mission capability until much needed performance improvements are developed, tested, and proven effective in testing representative of realistic LCS mine-clearance operations. Suspend further use of RMMV v6.0 until completing a comprehensive reliability-centered analysis, correcting

high impact failure modes, and testing repairs in an operationally realistic environment.

20. Given the cancelation of the RMS program, accelerate the development the most promising minehunting alternatives, including the USV with a towed AN/AQS-20C or AN/AQS-24C sensor and the Knifefish UUV with pre-planned product improvements.
21. Avoid overreliance on shore-based testing of mission package systems, which often results in unwarranted confidence in system performance in a maritime environment.
22. Fully resource the development of improvements to the ALMDS and AMNS (or alternative systems such as Barracuda). For ALMDS, efforts should focus on reducing the incidence of false contacts and eliminating the need for multi-pass search tactics. For mine neutralization systems, efforts should focus on reducing the incidents of fiber-optic communications losses, developing the ability to neutralize near-surface mines, and operating in high-current environments.
23. Demonstrate through end-to-end testing that the systems included in future mission packages can achieve the area search rate and detection/classification performance needed to support LCS effectiveness in timely and sustained minehunting and clearance operations. Testing should avoid segmented evaluations of individual components of the mission package.
24. Demonstrate viability of multi-ship LCS MCM Concept of Operations (CONOPS) that address operational concerns such as data sharing, contact management, asset scheduling, and mutual interference when multiple ships operate together to accelerate mine-clearance timelines and, since no planned version of the LCS MCM mission package is expected to perform all MCM functions, develop and demonstrate CONOPS for combined LCS and legacy MCM operations.
25. Accelerate development and production of the Navy Instrumented Threat Target (NAVITTAR) to ensure that sufficient resources are available to support planned developmental and operational testing of UISS and the MCM mission package. Implement a reliability improvement program to mitigate the high failure rate of NAVITTARs observed in early testing.
26. Characterize the magnetic properties of additional U.S. test ranges to identify a second suitable location to execute UISS operational testing.
27. To mitigate the risk of poor operational performance in the LCS MCM mission package, the Navy should demonstrate UISS integration aboard LCS in developmental testing prior to the initial phases of LCS-based operational testing, planned in FY18.
28. Provide adequate funding for developing, integrating, and testing mine hunting and mine sweeping systems in the LCS MCM mission package to mature the MCM capabilities to meet mission requirements.

ASW Mission Package

29. Acquire a sufficient quantity of GTTs, when developed, to characterize the capability of each LCS variant with ASW mission package to defeat threat torpedoes during operational assessment.

Future Operational Testing

30. Develop an operationally realistic, cost-effective alternative for training and testing of small-boat defense operations such as an accreditable, operator-in-the-loop simulation that incorporates tactical computing hardware and software and realistic threat presentations.
31. Provide adequate resources to conduct the full complement of test scenarios prescribed by the recently updated TEMP
32. Complete an update to the LCS TEMP to ensure that future tests, including integrated testing and plans for testing the over-the-horizon missile, are clear and resourced appropriately.
33. Fund development of test targets and ranges to adequately test LCS MCM systems, and then maintain and employ these assets to facilitate MCM operator training and proficiency after fielding.

MH-60S Multi-Mission Combat Support Helicopter

Executive Summary

- In FY16, in conjunction with delays in the Littoral Combat Ship (LCS) mine countermeasures (MCM) mission (MCM) package, the Navy delayed IOT&E of the MH-60S equipped with the Airborne Laser Mine Detection System (ALMDS) and the Airborne Mine Neutralization Systems (AMNS) until at least FY21. Since the Navy plans to declare Initial Operational Capability (IOC) of these systems in early FY17 and deploy them by FY18, prior to the completion of operational testing, DOT&E issued an early fielding report in June 2016. The report concluded that the MH-60S Airborne Mine Countermeasures (AMCM) helicopter equipped with ALMDS or AMNS would not be operationally effective or operationally suitable if called upon to conduct MCM missions in combat. The primary reasons for these conclusions are:
  - The combined AMCM systems are not reliable.
  - The ALMDS minehunting capabilities are limited in other-than-benign environmental conditions.
  - The AMNS cannot neutralize most of the mines in the Navy's threat scenarios.
  - The fleet is not equipped to maintain the ALMDS or the AMNS.
- DOT&E issued a classified FOT&E report in April 2014 that assessed the MH-60S Multi-spectral Targeting System (MTS) Automatic Video Tracker (AVT) does not adequately meet surface warfare (SUW) requirements. Currently, there are no prospective remediation modifications planned to address the system deficiencies that would likely enable it to meet SUW requirements. The Navy has shifted its focus to the long-term replacement for the HELLFIRE missile, the Joint Air-to-Ground Missile (JAGM), which employs a different guidance system that would obviate the need to correct the MTS AVT deficiencies.
- The Digital Rocket Launcher (DRL) with Advanced Precision Kill Weapon System (APKWS) II rockets, installed in response to an urgent operational need request, provides additional SUW capability to the MH-60S, but presents technical and operational risks that should be addressed for improved performance. Fielding the JAGM would also address the major shortcomings of the DRL with APKWS II.
- The Navy is currently procuring the Helmet Display and Tracking System (HDTS) on the MH-60S based solely on developmental testing. Current plans are to field the system without conducting operational testing.

System

- The MH-60S is a medium lift ship-based helicopter manufactured in three variants (blocks) that are derived from the Army UH-60L Blackhawk.
- All three blocks share a common cockpit, avionics, flight instrumentation, and power train with the MH-60R.
- Installed systems differ by block based on mission:
  - Block 1, Fleet Logistics – precision navigation and communications, maximum cargo or passenger capacity.
  - Block 2A/B, AMCM System – AMCM system operator workstation; a tether/towing system, two AMCM systems that the Navy plans to IOC in FY17 – ALMDS for detection and classification of near-surface mines and AMNS for neutralization of in volume and bottom mines – and a third system in early development, the Barracuda Mine Neutralization System, which the Navy expects to provide a near surface mine neutralization capability. The draft Capability Development Document hints that the Navy will integrate Barracuda with the MH-60S prior to the planned IOC in FY22. Any Block 2B or subsequent aircraft (e.g., Block 3 A/B aircraft) can be an AMCM aircraft.
  - Block 3A, Armed Helicopter – 20 mm Gun System, forward-looking infrared with laser designator, crew served side machine guns, dual-sided HELLFIRE air-to-ground missiles, the 2.75-inch family of rockets, and defensive electronic countermeasures.
  - Block 3B, Armed Helicopter – adds a tactical datalink (Link 16) to Block 3A capabilities.

Mission

The Maritime Component Commander can employ variants of MH-60S to accomplish the following missions:

- Block 1 – Vertical replenishment, internal cargo and personnel transport, medical evacuation, Search and Rescue, and Aircraft Carrier Plane Guard.
- Block 2 – Detection, classification, identification, and/or neutralization of sea mines, depending on the specific AMCM systems employed on the aircraft.
- Block 3 – Combat Search and Rescue, Surface Warfare, Aircraft Carrier Plane Guard, Maritime Interdiction Operations, Special Warfare Support, and detection, classification, identification, and/or neutralization of sea mines, depending on the specific AMCM systems employed on the aircraft.

Major Contractors

- Sikorsky Aircraft Corporation – Stratford, Connecticut
- Lockheed Martin Mission System and Sensors – Owego, New York

---

Activity

- In October 2015, the Navy delayed IOT&E of the *Independence*-variant LCS equipped with the first increment of the MCM mission package and its MH-60S AMCM systems pending the outcome of an independent review.
- In early 2016, following the completion of the independent review, the Navy announced plans to delay IOT&E of the LCS-based AMCM systems and declare an IOC for these systems in early FY17.
- In May 2016, DOT&E provided comments on the Navy's draft Capability Development Document for the Barracuda Mine Neutralization System. The Navy approved the Barracuda Mine Neutralization Capability Development Document in September 2016.
- In June 2016, DOT&E submitted an early fielding report to the Congress in response to the Navy's plan to deploy the *Independence*-variant LCS equipped with the MCM mission package, including the MH-60S with ALMDS and with AMNS, prior to the conduct of operational testing. The classified report, which does not support the Full-Rate Production decision, provided DOT&E's interim assessments of operational effectiveness and operational suitability of the *Independence*-variant LCS employing the MCM mission package and the AMCM systems.
- In 2016, the Navy reallocated funding intended to support near-term development of ALMDS pre-planned product improvements. The Navy also reported that the modified system would not be available to the LCS MCM mission package until at least FY21, thus indicating it will not be available in time to support the planned LCS MCM mission package IOT&E.
- In September 2016, the Navy announced that it plans to use fleet exercises to gather additional data to characterize previously unknown attributes of the AMCM systems it plans to IOC in FY17. For ALMDS, the Navy expects to characterize the system's probability of detection and classification as a function of mine spacing and water depth. For AMNS, the Navy expects to characterize performance of the system against buried mines.

Assessment

- The MH-60S AMCM helicopter, equipped with ALMDS or with AMNS, would not be operationally effective or operationally suitable if called upon to conduct MCM missions in combat. The primary reasons for these conclusions are:
  - The combined AMCM systems are not reliable.
  - The ALMDS minehunting capabilities are limited in other-than-benign environmental conditions.
  - The AMNS cannot neutralize most of the mines in the Navy's threat scenarios.
  - The fleet is not equipped to maintain the ALMDS or the AMNS.
- Since each LCS relies on a single helicopter to support all airborne MCM operations, MH-60S and AMCM mission kit reliability are critical factors affecting the timeliness of LCS-based MCM operations. Nonetheless, the Navy established a reliability requirement for the MH-60S (20.3 hours MTBOMF) but neglected to establish any requirements for the AMCM mission kit or for the combined AMCM system.
  - Based on data from combined developmental and integrated testing and operational assessments since 2011, MH-60S reliability is 26.3 hours MTBOMF, which exceeds the Navy's threshold requirement with high confidence. During the same period of testing, the average AMCM mission kit reliability is 24.5 hours MTBOMF; thus, its OMFs occur at approximately the same rate as MH-60S OMFs. The average reliability of the combined MH-60S AMCM helicopter is 12.7 hours MTBOMF, significantly less than the requirement for MH-60S reliability.
  - Mission kit reliability varies based on the AMCM mission configuration. On average, mission kit reliability is 59.1 hours MTBOMF during ALMDS missions and 19.0 hours MTBOMF during AMNS missions. The differing results are not surprising, since the MH-60S uses the AMCM tow cable and winch during AMNS missions but does not need these components during ALMDS missions. When the results are further merged with MH-60S reliability results, which vary little by mission

type, the combined MH-60S AMCM helicopter reliabilities are 16.9 hours MTBOMF during ALMDS missions and 10.7 hours MTBOMF during AMNS missions. Thus, the probability that the MH-60S and its mission kit can complete three 2.5-hour flights on any given day without experiencing a failure, which might be required during MCM operations, is 64 percent for ALMDS missions and 50 percent for AMNS missions. Those probabilities fall to 41 percent and 25 percent, respectively, for six 2.5-hour sorties on 2 consecutive days. Consequently, the probability of a single LCS sustaining high operating tempo AMCM missions is low.

- Since no operational testing of an AMCM-equipped MH-60S has occurred onboard an LCS, the LCS MCM TECHEVAL is the best source of data to assess the ability of ship and crew to sustain MH-60S AMCM operations. During the FY15 TECHEVAL, the MH-60S and its associated AMCM mission kit experienced nine problems that interrupted or delayed LCS MCM activities, nearly the same as the now canceled Remote Minehunting System (RMS). Operationally, the flight crew would have incurred at least one additional MH-60S AMCM delay because of an AMNS destructor launch failure that would have required aircrew to jettison the launch and handling system if live (explosive) neutralizers (operational assets) had been employed. Because of these problems, LCS 2 demonstrated sustained MH-60S AMCM operations lasting more than 1 week just once during TECHEVAL. Although the LCS Design Reference Mission suggests the MH-60S will operate daily in intervals of 10 to 12 days over several months, LCS 2 conducted MH-60S operations for 2 days or less on nine occasions during TECHEVAL before needing essential maintenance that in many cases required the ship or helicopter to return to port for spare parts or repairs.

• Although the Navy has taken action to mitigate ALMDS reliability problems observed in early testing, the system continues to experience occasional failures and, more often, nuisance faults that affect LCS AMCM operations. Over multiple periods of testing completed since 2012, system reliability has averaged 30.9 hours MTBOMF, exceeding the Navy's requirement of 25 hours MTBOMF. DOT&E did not include less-critical faults that interrupted missions only briefly or reduced the ALMDS search rate by 50 percent (because one or two of the four receivers were not functioning properly) in this calculation. However, a strict interpretation of the requirements document would count each of these faults as an additional OMF that would further reduce the reported reliability. Considering only the phases of testing completed after the Navy implemented an engineering change to mitigate the most common failure modes, ALMDS pods have experienced only one OMF in 74.4 hours of operations. However, each of the pods employed during this time completed less than 20 hours of lasing operations after the prime contractor groomed the system for testing. DOT&E cannot assess that the system is meeting its reliability requirement with confidence until it can verify that performance observed in these short periods is representative of sustained operations.

- The further combined results of MH-60S, AMCM mission kit, and ALMDS reliability suggest the integrated AMCM system experiences 1 OMF every 11.9 flight hours. Although the high failure rate of the combined system would make it difficult to sustain LCS-based operations, ALMDS pods have generally not been the primary source of mission downtime during stateside testing. Testers have also minimized ALMDS downtime during stateside testing by pre-positioning replacement systems to make them readily available in the event of a failure. This arrangement has produced high ALMDS availability results because testers assumed the system was available when at least one pod was operational, as opposed to recording uptime and downtime for each unit involved in the test. In the near-term, this approach is viable because the Navy has procured more ALMDS pods than deployable MCM mission packages; however, unless the Navy updates its ALMDS acquisition strategy to acquire additional units, it might not realize the same level of availability while operating more than a handful of MCM mission packages.
- Commander Task Force (CTF) 52 monitored the availability of individual ALMDS pods deployed to the Navy's Fifth Fleet area of responsibility in 2014 and reported that pods demonstrated an average operational availability of 62 percent compared to the Navy's requirement of 80 percent. Although the pods did not include the Navy's reliability improvements, root cause analysis determined that even if the Navy had implemented the engineering changes prior to deployment, they would not have prevented several failures responsible for significant downtime. CTF 52 also concluded that the lack of in-theater repair capability negatively affected ALMDS operational availability because of the need to transport pods to the contractor's facility in Melbourne, Florida, for intermediate- and depot-level repair. By eliminating transit time from the calculation, CTF 52 showed that ALMDS operational availability would improve to approximately 75 percent if a repair capability equal to that of the contractor's facility were available in theater.

• The Navy established two reliability requirements for the AMNS that address the system's LHS and neutralizer separately. The Navy's threshold requirements are 24 hours MTBOMF for the LHS and 0.85 for neutralizer reliability. Assessing compliance with the former requirement is challenging because the AMNS Capability Production Document does not define LHS operating time. Although the Navy often equates LHS operating time with MH-60S flight time, DOT&E limits its assessment of LHS operating time to the period during which the aircrew employs the system (e.g., from initial deployment to final retrieval).

- AMNS LHS reliability and neutralizer launch data show that on average, the LHS experiences one OMF for every 6.4 hours of operation and 17 neutralizer launches. Even if DOT&E used flight hours as the basis for its reliability calculation, LHS reliability would still be well short of the Navy's threshold. Moreover, the combined results of MH-60S, AMCM mission kit, and AMNS reliability suggest that the integrated AMCM system experiences one OMF every seven neutralizer launches and 5.9 flight hours, on average, during AMNS operations. By either measure, system reliability precludes timely and sustained operations.

- Neutralizer reliability is measured by the percentage of neutralizers launched that function as designed (i.e., give the operator an opportunity to identify and neutralize a mine) and is a component of the AMNS metric for probability of successful attack run. AMNS neutralizer reliability varies with environmental conditions, but is 65 percent, on average. Although the FY15 TECHEVAL produced the highest numerical result for neutralizer reliability, one should not attribute the change in the point estimate of neutralizer reliability to improvements in the underlying system. Instead, the combination of more favorable environmental conditions and the Navy's decision to avoid neutralizing most bottom targets, which had the highest incidence of failures in earlier testing, most likely led to the change in estimated performance between the operational assessment and the TECHEVAL. In addition to failures of the aircraft, mission kit, and LHS that delay completion of AMNS operations, multiple attempts to identify and neutralize the same contact (because of low neutralizer reliability) further extend AMNS and LCS MCM mission timelines.

- The ALMDS does not meet Navy detection/classification requirements. In particular, the system does not meet the Navy's requirements for minimum probability of detection and classification in all depth bins or the average probability of detection and classification in all conditions over a region of the water column that extends from the surface to a reduced maximum depth requirement. When the system and operator detect and classify a smaller percentage of mines than predicted by fleet planning tools, the MCM commander will likely underestimate the residual risk to transiting ships following clearance operations. To mitigate this uncertainty, the Navy might find it necessary to conduct follow-on minesweeping operations. However, the Navy does not plan to include the mechanical minesweeping capability that would be required in the MCM mission package. In some conditions, the system also generates a large number of false classifications (erroneous indications of mine-like objects) that can delay near-surface minehunting operations until conditions improve or slow mine clearance efforts because of the need for additional search passes to reduce the number of false classifications. In very favorable conditions, such as those observed during LCS MCM mission package TECHEVAL in FY15, detection performance meets the Navy's requirements and tactics, techniques, and procedures have been successful in reducing false classifications to the Navy's acceptable limits.
- The current increment of the AMNS has a system design limitation that prevents damage to the helicopter and is essential for the safety of aircrew. The current increment of the AMNS cannot neutralize mines that are moored above the system's prescribed operating ceiling, which will preclude neutralizing most of the mines expected in some likely threat scenarios; thus, alternative means, such as an Explosive Ordnance Disposal Team provided by another unit must be used to complete mine clearing. Within its operating range, AMNS performance is frequently degraded by the loss of fiber-optic communications between the aircraft and the neutralizer. The system has experienced loss of fiber-optic communications in a wide range of operationally relevant conditions, including those that are relatively benign. Although the Program Office has stated that it intends to develop an improved AMNS to extend its depth range and potentially improve performance in coarse bottom conditions and higher currents, none of these efforts are funded, and the Navy is considering needed Barracuda Mine Neutralization System capabilities that will compensate for shortfalls in AMNS operational performance.
- Consistent with the concept of operations, the LCS is reliant on shore-based support for assistance with diagnosis and repair of MCM mission systems including ALMDS and AMNS. The mission package detachment lacks the wherewithal to handle anything beyond relatively uncomplicated preventive maintenance and minor repairs. Thus, when ALMDS and AMNS failures occur, the Navy assumes that in most cases these systems will be replaced by embarked or shore-based spares.
- The MH-60S, as well as ALMDS and AMNS integrated on an LCS-based MH-60S have not completed cybersecurity testing.
- DOT&E's June 2016 early fielding report provides additional classified detail on MH-60S AMCM performance.
- DOT&E's classified April 2014 FOT&E report noted that the upgraded MH-60S MTS software showed some improved tracking performance compared to prior operational testing, but the MTS still did not meet its requirement for tracking. Additionally, the SUW mission capability of the MH-60S helicopter equipped with MTS and the HELLFIRE missile was not tested throughout the operational mission environment. Although the Navy is pursuing replacement of the AGM-114 HELLFIRE missile with the JAGM, which would obviate the need to correct the MTS deficiencies, the Milestone C decision for procuring JAGM is scheduled for late FY17 at the earliest. MTS tracking risks should be addressed as soon as possible. Failing to do so has left the Navy with a significant current capabilities gap in SUW that remains unaddressed. Should the JAGM fail to perform to requirements, this capabilities gap would continue to the foreseeable future with no alternative solution forthcoming.
- During FY14, a Quick Reaction Assessment of the MH-60S equipped with the DRL and APKWS II rockets demonstrated additional SUW capability for the MH-60S but identified technical and operational risks that should be addressed for improved mission performance. The preceding discussion on JAGM is also germane for the DRL with APKWS II.

Recommendations

- Status of Previous Recommendations. The Navy has partially addressed the FY11 recommendation to investigate solutions and correct the ALMDS False Classification Density and reliability deficiencies prior to IOT&E. The Navy has partially addressed the FY12 recommendation to assess corrections made to resolve previously identified MTS deficiencies by conducting FOT&E. The Navy has not acted or has yet to complete action on FY13, FY14, and FY15 recommendations:
  1. Complete comprehensive survivability studies for MH-60S employing the 20 mm Gun System and 2.75-inch Unguided Rockets.
  2. Conduct comprehensive live fire lethality testing of the HELLFIRE missile against a complete set of threat-representative small boat targets.
  3. Correct the tracking deficiencies in the MTS and conduct appropriate FOT&E in order to satisfactorily resolve the SUW Critical Operational Issue.
  4. Complete comprehensive IOT&E on the 2.75-inch Unguided Rocket and APKWS II to resolve the SUW Critical Operational Issue not resolved in limited assessments of system performance provided in Quick Reaction Assessments against small boat threats.
  5. Test the SUW mission capability of the MH-60S helicopter equipped with MTS and the HELLFIRE missile throughout the operational mission environment in FOT&E and LFT&E.
  6. Complete vulnerability studies for MH-60S employing the LAU-61G/A DRL armed with APKWS II rockets.
  7. Conduct comprehensive lethality testing of the LAU-61G/A DRL armed with APKWS II rockets against a complete set of threat-representative small boat targets.
  8. Correct AMCM mission kit reliability issues that limit AMNS mission availability identified during the operational assessment.
  9. Develop corrective actions to eliminate early termination fiber-optic communications losses observed in the AMNS operational assessment.
  10. Conduct AMNS medium current testing from MH-60S.
  11. Provide LCS with a mine neutralization capability in water depths above the current AMNS operating ceiling.
- FY16 Recommendations. The Navy should address the prior recommendations and consider the following actions:
  1. Conduct a comprehensive LCS-based cybersecurity assessment of the MH-60S helicopter with ALMDS and with AMNS.
  2. Limit procurement of ALMDS and AMNS, which are not meeting the Navy's original requirements and negatively affect LCS MCM capability, until much needed performance improvements are developed, tested, and proven effective in testing representative of realistic LCS mine-clearance operations.
  3. Fully resource the development of improvements to the ALMDS and AMNS (or alternative systems such as Barracuda). For ALMDS, efforts should focus on improving probability of detection over all required depths and relevant operating conditions, reducing the incidence of false contacts, and eliminating the need for multi-pass search tactics. For mine neutralization systems, efforts should focus on reducing the incidents of fiber-optic communications losses, developing the ability to neutralize near-surface mines, and operating in high-current environments.
  4. Avoid overreliance on shore-based testing, which often results in unwarranted confidence in system performance that may not be achieved during shipboard operations.
  5. Demonstrate through end-to-end testing that the systems included in future mission packages can achieve the area search rate and detection/classification performance needed to support LCS effectiveness in timely and sustained minehunting and clearance operations. Testing should avoid segmented evaluations of individual components of the mission package.

Mine Resistant Ambush Protected (MRAP) Family of Vehicles (FoV) – Marine Corps

Executive Summary

- In FY16, the Marine Corps completed live fire testing of the Mine Resistant Ambush Protected (MRAP) Cougar Category (CAT) II A1 with the Seat Survivability Upgrade (SSU). Preliminary analysis of the data indicates that the upgraded seats provide improved survivability over previous variants; the SSU provides force protection at the MRAP Capability Production Document (CPD) 1.1 objective level. DOT&E will provide a more comprehensive force protection/survivability evaluation in a final report in FY17.
- The program integrated approximately 100 SSU kits on CAT II A1 vehicles out of a planned total of 300.
- The Marine Corps is planning to retrofit all retained Cougar variants with egress upgrades, which will include power-assisted front and rear doors, redesigned rear steps, and a reconfigured exhaust system.
- In FY16, the Marine Corps completed live fire testing of the egress upgrades. The Cougar's power-assisted front doors did not function as designed post-event against CPD 1.1 objective-level threats; the vehicle's doors jammed during live fire testing. The program is investigating the vehicle structure to determine an appropriate solution.

System

- The MRAP Family of Vehicles (FoV) consists of medium-armored, all-wheel drive, tactical wheeled vehicles designed to provide protected mobility for personnel in a threat environment. Relative to the High Mobility Multi-purpose Wheeled Vehicle, MRAPs provide improved crew protection and vehicle survivability against current battlefield threats, such as IEDs, mines, small arms fire, rocket-propelled grenades, and explosively formed penetrators.
- The Marine Corps is retrofitting Cougar CAT II A1 vehicles with an SSU for improved survivability. The SSU integrates energy attenuating seats into the rear crew compartment and reconfigures the Automatic Fire Extinguishing System and internally stowed equipment.
- The Marine Corps is assessing egress upgrades to the Cougar FoV. The egress upgrade consists of new power-assisted front and rear doors, redesigned rear steps, and a reconfigured exhaust system.
- The Marine Corps will retain 2,500 MRAP vehicles in its enduring fleet: 68 Buffalo, 1,727 Cougar (CAT I, CAT II, and Ambulance), and 705 MRAP – All Terrain Vehicle. The Marine Corps will remain the Primary Inventory Control Activity for all Cougar platforms, including those vehicles divested to the Navy and Air Force.

Mission

Commanders will employ Marine units equipped with the MRAP Cougar to conduct mounted patrols, convoy protection, reconnaissance, communications, and command and control missions to support combat and stability operations in highly-restricted rural, mountainous, and urban terrain.

Major Contractor

General Dynamics Land Systems – Ladson, South Carolina

Activity

- The program completed the Cougar CAT II A1 with SSU live fire testing at Aberdeen Test Center (ATC), Maryland, in June 2016 in accordance with the DOT&E-approved test plan.
- The program completed five live fire egress test events along with exploitation testing, on a range of Cougar variants, at ATC from June through August 2016. These tests were completed in accordance with the DOT&E-approved test plan.
- In FY16, the program integrated approximately 100 SSU kits on CAT II A1 vehicles out of a planned total of 300.
- The program is investigating solutions to the floor and hull to further improve Cougar CAT II A1 survivability/force protection by modifying the structural response of the vehicle. The effort is using modeling and simulation to select potential designs.

Assessment

- The preliminary analysis of live fire test data indicate the Cougar CAT II A1 with the SSU provides force protection at the MRAP CPD 1.1 objective level. The upgraded seats demonstrated improved protection over previous variants against underbody mines while not degrading performance relative to other previously tested threats such as fragmenting IEDs, indirect fire, small arms fire, rocket-propelled grenades, and explosively-formed penetrators. DOT&E will provide a more comprehensive force protection/survivability evaluation in a final report to Congress in FY17.
- The Cougar's power-assisted doors did not function as designed post-event against CPD 1.1 objective-level threats. The vehicle's doors jammed during live fire testing. The program is investigating the vehicle structure to determine an appropriate the solution.

Recommendations

- Status of Previous Recommendations. The program has addressed the previous recommendation regarding upgrading the seats in the Cougar A1 vehicles.
- FY16 Recommendations.
    1. The Marine Corps should implement a fix to the front door problem encountered during egress upgrade testing at the contract threshold level, and conduct a follow-on event to verify threshold-level performance.

MK 54 Lightweight Torpedo and Its Upgrades Including High Altitude Anti-Submarine Warfare Capability

Executive Summary

- The Navy continued development of hardware and software updates to the MK 54. The new version, designated the MK 54 Mod 1 torpedo, is scheduled to begin OT&E in FY20.
- The Navy started the MK 54 Mod 1 development in FY07 and in-water developmental testing in November 2015. The Navy has completed 16 of the planned 80 MK 54 Mod 1 developmental test firings and obtained valid test data from 11. In February 2016, the Navy paused the second of six in-water developmental test events to search for two lost test torpedoes. The Navy updated its developmental test plans and resumed the in-water developmental test program in October 2016.
- In February 2016, the Navy completed a Milestone C acquisition decision for the MK 54 Mod 1 without a Navy-approved Capability Development Document or an approved Test and Evaluation Master Plan (TEMP). The Navy approved the MK 54 Mod 1 Capability Development Document on September 26, 2016.
- The High-Altitude Anti-Submarine Warfare Weapons Capability (HAAWC) program, designed to deliver the MK 54 torpedo from the cruising altitude of a P-8A aircraft, began initial contractor flight testing and initial P 8A Poseidon Flight Clearance safety testing in FY16. The Navy has not approved a requirements document yet for the HAAWC.
- Based on data collected in the Navy's scaled MK 54 warhead tests executed in FY16, it is assessed the MK 54 will remain not effective even with the Mod 1 fixes. Details supporting this assessment will be provided in a classified LFT&E report that will be issued in FY17.

System

- The MK 54 Lightweight Torpedo is the primary anti-submarine warfare (ASW) weapon used by U.S. surface ships, fixed-wing aircraft, and helicopters. The MK 54 must interoperate and be compatible with the analog or digital combat control systems and software variants installed on all ASW fixed-wing and helicopter aircraft, and on the surface ship combat control system variants used for torpedo tube or ASW rocket-launched torpedoes.
- The MK 54 combines the advanced sonar transceiver of the MK 50 torpedo with the legacy warhead and propulsion system of the older MK 46. MK 46 and MK 50 torpedoes are converted to an MK 54 via an upgrade kit.
- The Navy designed the MK 54 to operate in shallow-water environments and in the presence of countermeasures. The MK 54 sonar processing uses an expandable, open architecture system. It combines algorithms from the MK 50 and MK 48 torpedo programs with commercial off-the-shelf technology.

- The Navy has designated the MK 54 torpedo to replace the MK 46 torpedo as the payload section for the Vertical Launched Anti-Submarine Rocket for rapid employment by surface ships.
- The MK 54 Block Upgrade (BU) was a software upgrade to the MK 54 baseline torpedo designed to provide a small, shallow draft target capability and to correct deficiencies identified during the 2004 MK 54 IOT&E.
- The Navy is developing the MK 54 Mod 1. The MK 54 Mod 1 hardware upgrades the torpedo's sonar array from 52 to 112 elements, providing higher resolution. Associated software upgrades are designed to exploit these features to improve target detection and enhance false target rejection as well as correct previously identified deficiencies.
- The HAAWC will provide an adapter wing-kit to permit long-range, high-altitude, GPS-guided deployment of the MK 54 by a P-8A Multi-mission Maritime Aircraft. A follow-on capability to receive in-flight targeting updates via Link-16 from the P-8A is expected to be added in a later program phase. In-flight updates will not be available in the baseline HAAWC kit.

Mission

Commanders employ naval surface ships and aircraft equipped with the MK 54 torpedo to conduct ASW:
- For offensive purposes, when deployed by ASW aircraft and helicopters
- For defensive purposes, when deployed by surface ships
- In both deep-water open ocean and shallow-water littoral environments
- Against fast, deep-diving nuclear submarines and slow-moving, quiet, diesel-electric submarines

Major Contractors
- Raytheon Integrated Defense Systems – Tewksbury, Massachusetts
- Progeny Systems Corporation – Manassas, Virginia
- Boeing Company – St. Charles, Missouri
- Northrop Grumman – Annapolis, Maryland

Activity
- During FY16, the Navy continued development of new MK 54 Mod 1 torpedo front-end hardware and tactical software to address the performance shortfalls identified with the MK 54 (BU). The Navy plans to begin the MK 54 Mod 1 OT&E in FY20.
- The Navy began MK 54 Mod 1 development in FY07 and started in-water developmental testing in November 2015. The Navy's developmental test plan called for firing 80 MK 54 torpedoes in 6 separate test events covering both deep and shallow water scenarios, between September 2014 and May 2016. During the November 2015 test event, the Navy fired 10 MK 54 Mod 1 torpedoes in deep water scenarios and obtained valid test data from 8 torpedoes. During the February 2016 test event, the Navy fired 6 of the 10 planned MK 54 Mod 1 torpedoes before pausing the in-water test event to search for two lost test torpedoes. The Navy updated its developmental test plans and resumed the in water developmental test program in October 2016.
- In February 2016, the Navy completed a Milestone C acquisition decision for the MK 54 Mod 1 without a Navy-approved Capability Development Document or an approved TEMP. DOT&E continues to work with the Navy's Operational Test and Evaluation Force and the Program Office to develop an adequate MK 54 Mod 1 operational test program within the constraints of the available test target surrogates. The Navy approved the MK 54 Mod 1 Capability Development Document on September 26, 2016, but that document did not address the HAAWC program that has started testing. The Navy is developing a separate requirements document to address that program.
- In FY15, DOT&E participated in the Navy's Torpedo Target Strategy Working Group to identify and develop test target surrogates for the MK 54. The Navy proposed a short-term strategy that utilizes three separate torpedo targets, each appropriate for specific limited scenarios. However, the Navy did not fund the short-term strategy and has not developed a long-term target strategy.
- In FY15 and FY16, DOT&E funded and participated in two Resource Enhancement Program projects to develop critical assets for torpedo operational testing. One project develops the Submarine Launched Modular 3-inch Device (SLAM-3D) as a threat-representative surrogate torpedo countermeasure. The second project is an update to the Weapons Assessment Facility (WAF) hardware-in-the-loop modeling and simulation testbed located at the Naval Undersea Warfare Center in Newport, Rhode Island. The project is intended to improve the WAF for developing and testing torpedoes by improving the modeling of the ocean environment and improving target models.
- In FY16, Boeing continued contractor testing of the HAAWC wing kits for employing the MK 54 torpedo from the P-8A at medium to high altitudes. The Navy started initial integration testing and initial flight clearance safety testing of the HAAWC into the P-8A Poseidon aircraft.
- As a result of increased HAAWC program cost estimates and reduced funding, the Navy transferred sponsor organizational responsibilities within the Navy staff and is revising performance thresholds, which it is documenting in a draft HAAWC Capabilities Production Document.
- The HAAWC program has not yet developed a comprehensive test strategy and does not have an approved TEMP. The HAAWC program is scheduled to begin OT&E in FY19. DOT&E continues to work with the Navy to develop an adequate operational test strategy.
- In September 2015, the Navy conducted a small-scale test of the warhead to characterize hull deformation as a function of weapon standoff. The Navy has not delivered the final report on this test series. The results of the small-scale test were used to plan a large-scale test executed in late FY16, which the Navy performed at Aberdeen Test Center, Underwater Explosion Test Facility, using a scaled MK 54 warhead against a threat-representative target. The primary objective of this testing was to demonstrate weapon lethality by quantifying the extent of damage and hull rupture to the target hull.

Assessment
- In FY14, DOT&E assessed that the MK 54 torpedo is not operationally effective as an offensive ASW weapon. During operationally challenging and realistic scenarios, the MK 54 (BU) demonstrated below threshold performance and exhibited many of the same failure mechanisms observed during the IOT&E. Torpedo mission kill performance against targets

employing operationally realistic evasion tactics was below requirement thresholds. Performance was further degraded when considering crew performance for targeting and employing the MK 54 (BU) and the Navy's assessment of the warhead. The Navy designed the MK 54 Mod 1 upgrade to improve the MK 54's hit performance in these test scenarios.
- DOT&E also reported the MK 54 (BU) torpedo was operationally suitable and met the same reliability and availability requirements as the baseline torpedo. However, MK 54 (BU) operational testing identified shortfalls with the employing platforms' tactics and tactical documentation, and interoperability problems with some platform fire control systems. The Navy initiated immediate actions to address these shortfalls and has reported the training and tactics shortfalls are fixed for the MK 54 (BU). DOT&E plans to evaluate the effectiveness of the employing platforms' tactics, documentation, and interoperability during the MK 54 Mod 1 OT&E.
- Some MK 54 (BU) operational realistic scenarios were not assessed due to the unavailability of target surrogates and the Navy's safety regulations for shooting against manned submarine targets. Due to resource constraints, the Navy has not developed adequate set-to-hit surrogate targets and test articles. Because of these test limitations, the Navy will not be able to assess MK 54 Mod 1 performance in all important operationally realistic scenarios. DOT&E plans to conduct set-not-to-hit testing with manned submarines and limited set-to-hit testing with available target surrogates to assess if the MK 54 Mod 1 improves hit performance and corrects MK 54 (BU) shortfalls. These test limitations will result in an upper bound estimate of MK 54 hit performance but are acceptable for Mod 1 testing given past performance shortfalls. However, the Navy must fund efforts to resolve these test limitations.
- The Navy intends the MK 54 Mod 1 to improve MK 54 (BU) effectiveness with a new 112-element hydrophone front end, new processors, and new software designed to improve detection, classifier, and tracker performance. Completed developmental testing demonstrated performance results similar to the MK 54 (BU); however, to date, the Navy has conducted most developmental testing using simple structured scenarios where the MK 54 previously demonstrated satisfactory performance. These simple developmental test scenarios are good regression testing that yield significant recorded test data; however, little data were obtained to assess MK 54 performance in challenging, operationally realistic scenarios. The Navy is planning additional in-water developmental testing to assess more challenging operational scenarios.
- Based on data collected in the Navy's scaled MK 54 warhead tests executed in FY16, it is assessed the MK 54 will remain not effective even with the Mod 1 fixes. Details supporting this assessment will be provided in a classified LFT&E report that will be issued in FY17.

Recommendations
- Status of Previous Recommendations. The following previous recommendations remain outstanding. The Navy still needs to:
  1. Conduct operationally realistic mobile target set-to-hit testing scenarios. The Navy has not developed a mobile target surrogate for set-to-hit testing. The Navy investigated possible surrogates; however, the proposals are unfunded.
  2. Propose alternatives to minimize or eliminate the test and safety limitations that minimize operational realism in MK 54 testing.
  3. Complete development of the MK 54 Mod 1 TEMP.
  4. The Navy should evaluate and incorporate the 11 recommendations in DOT&E's MK 54 (BU) OT&E report to improve the effectiveness of the MK 54. Significant unclassified recommendations include:
     - Improve the target detection localization and track performance of ship and aircraft crews that employ the MK 54. While improving the sensor system capability on ships and aircraft is a longer range goal, updating the MK 54 employment tactics, training, and documentation could immediately improve overall crew proficiency and ASW effectiveness. The Navy has reported it has made progress in updating its tactics and documentation, but there has been no testing yet to verify the deficiencies have been resolved.
     - Improve the MK 54's effective target search and detection capability. The MK 54 should be able to effectively search the area defined by typical fire control solution accuracy and crew employment and placement errors.
     - Reduce the complexity of the MK 54 employment options and required water entry points in existing tactical documentation. The Navy has reported it has made progress in updating its tactics and documentation, but there has been no testing yet to verify the deficiencies have been resolved.
- FY16 Recommendations. The Navy should:
  1. Complete the development and approval of the HAAWC requirements and TEMP.
  2. Utilize developmental test scenarios that stress the MK 54 Mod 1 in scenarios where improvements are desired. When possible, these scenarios should be operationally realistic.
  3. Initiate recommendations that will be provided in the FY17 MK 54 LFT&E report.

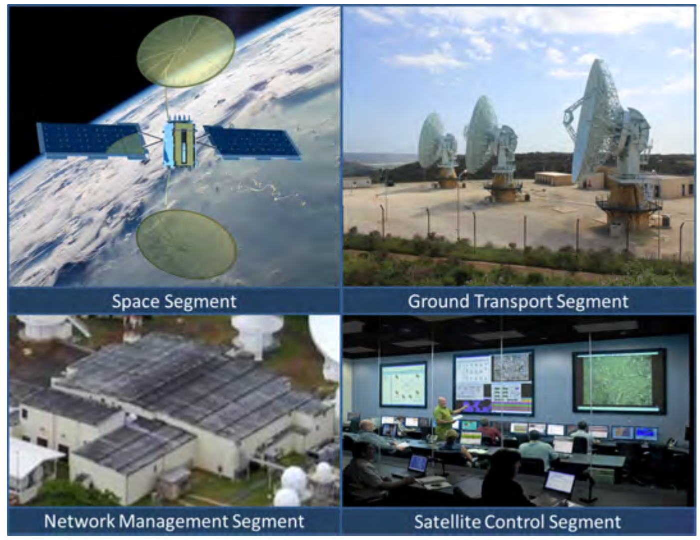
Mobile User Objective System (MUOS)

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted the Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation 2 (MOT&E 2) from October 19 through November 20, 2015. DOT&E approved the Test and Evaluation Master Plan (TEMP) on November 29, 2010, and the MOT&E 2 test plan on October 13, 2015.
- MUOS is not operationally effective in providing reliable worldwide Wideband Code Division Multiple Access (WCDMA) communications to tactical users. MUOS was able to provide WCDMA communications on a limited scale during MOT&E 2, but MUOS cannot achieve this performance worldwide given the significant problems with planning and provisioning, situational awareness, network management, and capacity.
- MUOS is not operationally suitable. The ground system lacks the stability and maturity to enter into and sustain global operations. MUOS does not provide communications that deployed users can rely on when the system is in widespread use or at full capacity. MUOS performed poorly in almost every area of operational suitability.
- The system is not survivable against cyber-attacks. The COTF Red Team and U.S. Strategic Command (USSTRATCOM) conducted independent cyber assessments and obtained similar results. They discovered over 1,000 cybersecurity vulnerabilities in the MUOS ground system.
- MUOS is not ready to support military operations. Until the problems are fixed and verified in the FOT&E, the system use should be limited to small non-combat missions, testing, training, and exercises in the United States and protectorates in order to develop, exercise, and mature operational concepts and processes with a particular focus on addressing known issues and MOT&E-2 findings.
- The Navy launched the MUOS-5 on-orbit spare satellite on June 24, 2016. On June 29, the Navy discovered an anomaly during orbit-raising. The satellite is safe and remains in a stable interim orbit while the Navy evaluates options.
- On July 18, 2016, the Commander, USSTRATCOM accepted for Early Combatant Command Use the MUOS capability, consistent with the DOT&E recommendation.

System

- MUOS is a satellite-based communications network designed to provide worldwide, narrowband, beyond line of-sight, point-to-point, and netted communication services to multi Service organizations of fixed and mobile terminal users. The Navy designed MUOS to provide 10 times the throughput capacity of the current narrowband satellite communications.



The Navy intends for MUOS to provide increased levels of system availability over the current constellation of Ultra High Frequency (UHF) Follow-On satellites and to improve availability for small, disadvantaged terminals.

- MUOS consists of six segments:
  - The Space Segment consists of four operational satellites and one on-orbit spare. Each satellite hosts two payloads: a legacy communications payload that mimics the capabilities of a single UHF Follow-On satellite and a MUOS communications payload.
  - The Ground Transport Segment is designed to manage MUOS communication services and allocation of radio resources.
  - The Network Management Segment (NMS) is designed to manage MUOS ground resources and allow for government-controlled, precedence-based communication planning.
  - The Ground Infrastructure Segment is designed to provide transport of both communications and command and control traffic between MUOS facilities and other communication facilities.
  - The Satellite Control Segment consists of MUOS telemetry, tracking, and commanding facilities at the Naval Satellite Operations Center Headquarters and Detachment Delta.
  - The User Entry Segment provides a MUOS waveform hosted on MUOS-compatible terminals. The Army's Project Manager for Tactical Radios is responsible for developing and fielding MUOS-compatible terminals. The Air Force, Navy, and Marine Corps are upgrading legacy UHF radios to be MUOS-compatible.

Mission

Combatant Commanders and U.S. military forces deployed worldwide will use the MUOS satellite communications system to accomplish globally assigned operational and joint force component missions, especially those involving highly mobile users. Such missions include major conventional war; regional conflicts; search and rescue; humanitarian or disaster relief (including severe weather events); homeland security; homeland defense; counterterrorism; non-combatant; evacuation operations; very important person travel; strategic airlift; global mobility; global strike; intelligence, surveillance, and reconnaissance; training; logistics support; and exercise support.

Major Contractors

- Lockheed Martin Space Systems – Sunnyvale, California
- General Dynamics C4 Systems – Scottsdale, Arizona

Activity

- The Navy conducted a government Developmental Test Technical Evaluation from June 1 – 30, 2015, in preparation for operational testing.
- COTF conducted MOT&E 2 from October 19 through November 20, 2015, in accordance with the approved TEMP and test plan. DOT&E approved the TEMP on November 29, 2010, and the MOT&E 2 test plan on October 13, 2015.
- COTF conducted a two-phase cybersecurity assessment of the MUOS system in conjunction with MOT&E 2. COTF conducted the phase one Cooperative Vulnerability and Penetration Assessment in November 2015 and a phase two Adversarial Assessment in April 2016.
- DOT&E submitted a report in June 2016, evaluating the system based on MOT&E-2.
- The program manager requested a deferral of the geolocation capability from MOT&E 2. Geolocation is the ability to locate a legacy UHF electromagnetic interferer on the ground.
- The Navy launched the MUOS-5 on-orbit spare satellite on June 24, 2016. On June 29, the Navy discovered an anomaly during orbit-raising. The satellite is safe and remains in a stable interim orbit while the Navy evaluates options.
- On July 18, 2016, the Commander, USSTRATCOM accepted for Early Combatant Command Use the MUOS capability, consistent with the DOT&E recommendation.
- The MUOS program manager and COTF have begun updating the previous TEMP to encompass the scope of the next operational test, planned for FY18 or FY19.

Assessment

- When MUOS works, it provides message accuracy and quality of service better than legacy UHF communications. However, MUOS cannot communicate on all types of group network services. COTF did not test fixed assigned networks because of known problems with them.
- MUOS does not meet the threshold capacity Key Performance Parameter criteria, based on the two satellite configurations in MOT&E-2. The 2 satellites under test operated at 72 percent of capacity during MOT&E-2. DOT&E determined that 92 of the possible 128 satellite beam carriers were active on the Pacific and Continental United States region satellites, for an availability of 71.9 percent. The Navy either locked or turned off 28.1 percent of the capacity to prevent problems with interference from ambient radio frequency signals. A locked satellite beam carrier means users cannot access it, effectively losing 5 megahertz of potential spectrum in that beam. A majority (56 percent) of 32 satellite beams across the two satellites were in a degraded mode.
- During MOT&E 2, resource planners were able to obtain information from the system in 61 percent (52 of 85) of attempts. USSTRATCOM cannot monitor MUOS and evaluate actual system performance against planned performance. MUOS does not provide USSTRATCOM with an accurate, real-time status of the system state. The system was unable to maintain call records for the 60 terminals that participated in MOT&E-2.
- The ability of MUOS to create, analyze, and implement communications plans has problems. The system occasionally freezes when analyzing what network resources are available and the network data are sometimes inaccurate. Without a valid and accurate plan, MUOS cannot create configurations for all of the radios and users cannot establish communications with one another.
- The MUOS fault management system is ineffective because it provides the network managers fault alarm events that are cryptic, inconsistently prioritized, and often excessive. The filtering effort was incomplete and arbitrary.
- During developmental and operational test periods, hardware failures at the MUOS Radio Access Facilities have led to the loss of as much as half of the communications resources on a single satellite. MUOS does not provide a proactive means to monitor WCDMA communication failures, resulting in potentially extended outages for deployed users. The MUOS network managers cannot assess and report on WCDMA satellite beam carrier availability. Key systems associated with WCDMA call services, such as the radio base stations in the Radio Access Facilities, do not provide fault information to the fault management system. The program manager is working on a solution to provide improved situational awareness.
- MUOS was able to conduct routine Over-the-Air Rekeys but cannot reliably conduct compromised terminal operations. The reliability problems could result in global communications outages for an entire military Service or all Special Operations units. An outage would persist until its root cause is resolved

and the MUOS ground system broadcasts an updated cryptographic key.

- The NMS was often not operationally available. The NMS was available 6.3 percent of the time during MOT&E-2 against a 95 percent threshold criterion. The NMS had long repair times, numerous high-priority problem reports, poor usability, poor documentation, and high reliance on depot maintainers. Additionally, NMS is undermanned and operators do not consider themselves adequately trained to perform their mission. Multiple failures in the NMS and the Ground Transport Segment during MOT&E-2 created long communications outages.
- During MOT&E-2, there were over 200 high-priority hardware and software problems remaining on the system.
- The geolocation capability is still in development and was deferred from MOT&E 2. The program manager is developing a geolocation capability which will need to be operationally tested in the planned FOT&E.
- MUOS is not operationally effective in providing reliable worldwide WCDMA communications to tactical users. MUOS was able to provide WCDMA communications on a limited scale during MOT&E 2, but MUOS cannot achieve this performance worldwide given the significant problems with planning and provisioning, situational awareness, network management, and capacity.
- MUOS is not operationally suitable. The ground system lacks the stability and maturity to enter into and sustain global operations. MUOS does not provide communications that deployed users can rely on when the system is in widespread use or at full capacity. MUOS performed poorly in almost every area of operational suitability.
- The system is not survivable from cyber-attacks. The COTF Red Team and USSTRATCOM conducted independent cybersecurity assessments and obtained similar results. They discovered over 1,000 cybersecurity vulnerabilities in the MUOS ground system. Approximately half of these vulnerabilities are Category-II and above. Category-II vulnerabilities have a high potential of giving system access to an intruder.
- MUOS is not ready to support military operations. Until the problems are fixed and verified in the FOT&E, the system's use should be limited to small non-combat missions, testing, training, and exercises in the United States and protectorates in order to develop, exercise, and mature operational concepts and processes with a particular focus on addressing known issues and MOT&E-2 findings.
- The Commander, USSTRATCOM decision for Early Combatant Command Use of the MUOS capability will benefit Service members and assist the MUOS program manager in resolving system problems while providing the operational manager, provisioners, and network managers with valuable experience through limited operations.
- The program manager, in coordination with USSTRATCOM, is evaluating courses of action to resolve the anomaly with the MUOS-5 on-orbit spare satellite. They continue to analyze the situation, consider alternate orbit adjustment options, and assess mission impacts.

Recommendations

- Status of Previous Recommendations. The Navy is in the process of updating the TEMP for the planned FOT&E.
- FY16 Recommendation.
  1. The Navy should provide resources to address the recommendations in the DOT&E MOT&E-2 report prior to the FOT&E. COTF should verify the corrections in the FOT&E.

MQ-4C Triton Unmanned Aircraft System

Executive Summary

- The Navy conducted an Operational Assessment (OA) from November 2015 through January 2016. Testing was completed in accordance with the DOT&E-approved test plan. In general, the system demonstrated positive trends for sensor performance and reliability during the OA. The maximum detection and classification ranges for maritime targets exceeded Capability Development Document requirements and the Triton crews were able to transmit Electro-optical/Infrared (EO/IR) video to the Surface/Aviation Interoperability Lab via Common Data Link. The system reliability is currently tracking the Reliability Growth Curve annotated in the System Engineering Plan and the Test and Evaluation Master Plan (TEMP). However, the OA revealed deficiencies in the following areas: lack of Due Regard capability (capability to independently maintain prescribed minimum separation distances); poor EO/IR sensor control; poor Electronic Support Measures operator interface; and difficulty managing the temperature of the radar.
- DOT&E published the classified OA report in May 2016, and approved the MQ-4C TEMP in April 2016, to support the Milestone C decision which occurred in August 2016.

System

- The MQ-4C Triton UAS is an intelligence, surveillance, and reconnaissance system-of-systems consisting of the high-altitude, long-endurance MQ-4C air vehicle, sensor payloads, and supporting ground control stations. The MQ-4C system is a part of the Navy Maritime Patrol and Reconnaissance family-of-systems and will provide multiple types of surveillance data over vast tracks of ocean and littoral areas; overland intelligence, surveillance, and reconnaissance; signals intelligence and target acquisition capabilities designed to complement the P-8A Poseidon Multi-mission Maritime Patrol aircraft.
- The MQ-4C air vehicle design is based on the Air Force RQ-4B Global Hawk air vehicle with significant modifications that include strengthened wing structures and an anti-ice and de-icing system.
- Mission systems include a maritime surveillance radar to detect, identify, and track surface targets and produce high-resolution imagery.
  - An EO/IR sensor provides full motion video and still imagery of surface targets and the Electronic Support Measures system detects, identifies, and geolocates threat radar signals.
  - An Automatic Identification System (AIS) receiver permits the detection, identification, geolocation, and tracking of cooperative maritime vessels equipped with AIS transponders.
- Planned future system upgrades include an air traffic collision avoidance radar system and a signals intelligence collection system. Onboard line-of-sight and beyond line-of-sight datalink and transfer systems provide air vehicle command and control and transmit sensor data from the air vehicle to ground control stations for dissemination to fleet tactical operation centers and intelligence exploitation sites.

Mission

- Commanders employ units equipped with MQ-4C to conduct long-endurance maritime surveillance operations and provide high- and medium-altitude intelligence collection.
  - MQ-4C operators will detect, identify, track, and assess maritime and littoral targets of interest and collect imagery and signals intelligence information.
  - Operators disseminate sensor data to fleet units to support a wide range of maritime missions to include surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue.

Major Contractor

Northrop Grumman Aerospace Systems, Battle Management and Engagement Systems Division – Rancho Bernardo, California

Activity

- The Navy conducted an OA from November 2015 through January 2016. Testing was completed in accordance with the DOT&E-approved test plan. However, since the MQ-4C is not yet authorized to operate on Navy operational networks, the Navy did not accomplish a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) of the MQ-4C during the OA. DOT&E published the classified OA report in May 2016.
- DOT&E approved the MQ-4C TEMP in April 2016 to support of the Milestone C decision which occurred in August 2016.
- The program has changed its Acquisition Strategy and moved IOT&E from 4QFY17 to 4QFY20 to align with development and fielding of the Multiple Intelligence (Multi-INT) configuration. The Multi-INT configuration provides a signals intelligence capability, and includes sensors, supporting software and hardware, and changes to permit processing of Top Secret and Sensitive Compartmented Information. The Navy intends for the MQ-4C Multi-INT configuration to replace the EP-3 Aries II aircraft for most missions. The Navy plans to field two MQ-4C aircraft in the baseline configuration (non-Muti-INT) in FY18, prior to Initial Operational Capability (IOC), to provide an Early Operational Capability.
- The program continues to pursue a solution providing traffic de-confliction and collision avoidance capability since development of the Air-to-Air Radar Subsystem was stopped. The program intends to select a technical solution after IOC. The Navy is investigating alternative means of Due Regard compliance including procedures and other cooperative avoidance systems already integrated in the MQ-4C in order to support MQ-4C operations at IOC.

Assessment

- In general, the system demonstrated positive trends for sensor performance and reliability during the OA. The maximum detection and classification ranges for Maritime targets exceeded Capability Development Document requirements and the Triton crews were able to transmit EO/IR video to the Surface/Aviation Interoperability Lab via Common Data Link. The system reliability is currently tracking the Reliability Growth Curve annotated in the System Engineering Plan and the TEMP. However, the OA revealed deficiencies in the following areas: lack of Due Regard capability (capability to independently maintain prescribed minimum separation distances); poor EO/IR sensor control; poor Electronic Support Measures Interface; and difficulty managing the temperature of the radar. DOT&E's classified report provides specific information on these and other aspects of the assessment.
- Traffic de-confliction and collision avoidance (Due Regard capability) provides critical mission capability for operation of the MQ-4C in civil and international airspace in support of global naval operations. Any limitation to this capability at IOT&E will reduce the effectiveness of the MQ-4C.

Recommendations

- Status of Previous Recommendations. The Navy still needs to addressed the following DOT&E recommendations:
  1. Demonstrate any alternative means of compliance with the Due Regard requirement prior to IOT&E and conduct a CVPA sufficiently in advance of the Adversarial Assessment (AA) to allow the program to correct any discovered cybersecurity vulnerabilities;
  2. Conduct both the CVPA and AA prior to any early fielding of the MQ-4C.
- FY16 Recommendations. In addition to addressing the recommendations above, the Navy should:
  1. Resolve deficiencies documented in the DOT&E OA report prior to IOT&E, especially in the following areas: Due Regard capability; EO/IR sensor control; Electronic Support Measures Interface; temperature management of the radar.

MQ-8 Fire Scout

Executive Summary

- The Commander, Operational Test and Evaluation Force (COTF) and Air Test and Evaluation Squadron ONE (VX-1) conducted the land-based Quick Reaction Assessment (QRA) from May through June 2015 in response to a request by the Director, Battlespace Awareness, Operational Navy N2/N6F2, for an assessment of the operational capabilities and limitations of the radar-equipped MQ-8B Fire Scout to support maritime and littoral operations.
  - DOT&E assessed MQ-8B performance in a March 2016 memorandum to the Navy.
  - While this QRA demonstrated the potential of the radar-capable MQ-8B, this land-based-only QRA may have presented an overly optimistic assessment of this capability. The Navy intends for the radar-equipped MQ-8B to launch from a host vessel capable of supporting helicopter flight operations (such as the Littoral Combat Ship (LCS)) in support of intelligence and surface warfare (SUW) operations. This concept of operations was not demonstrated during the QRA.
- VX-1 conducted the MQ-8C operational assessment (OA) at Naval Air Station Point Mugu, California, in November 2015 to support the upcoming Milestone C decision. This testing focused on air vehicle endurance, mission coverage, performance of the MQ-8C electro-optical/infrared (EO/IR) sensor in a littoral environment, reliability of the system, and operator workloads.
  - DOT&E assessed MQ-8C performance in a June 2016 memorandum to the Navy.
  - The MQ-8C OA presents a partial assessment of MQ-8C performance. This land-based MQ-8C OA presents an overly optimistic assessment of the capability since the Navy did not complete shipboard testing under operational conditions.
- The Navy awarded a contract for 10 additional MQ-8C helicopters in September 2015 bringing the total number to 29. The Navy plans to complete their buy of the remaining 11 aircraft in FY17 prior to IOT&E.
- The Navy is planning to conduct the Milestone C decision for the restructured program in 2QFY17.

System

- The MQ-8B and follow-on MQ-8C are helicopter-based tactical unmanned aerial systems that support intelligence, surveillance, and reconnaissance (ISR), SUW, and mine countermeasures (MCM) payloads.
- The Navy plans to replace the MQ-8B airframe (Schweizer 333) with the MQ-8C airframe (Bell 407), which has better endurance and payload capacity. MQ-8B vehicles are deployed on ships in the fleet and will be phased out via attrition. The MQ-8C concept of operations is primarily in support of LCS missions but it can also be employed off other suitably equipped aviation capable ships.

MQ-8B

MQ-8C

- The MQ-8C airframe is equipped with the AN/AAQ-22D Bright Star II, a multi-sensor imaging system with EO/IR cameras and laser designation/range finding.
- The Navy plans to incrementally integrate different mission payloads into the MQ-8C airframe:
  - The Endurance Baseline Increment integrates the AN/AAQ-22D Bright Star II, Automated Identification System (AIS), Tactical ISR (TAC-ISR) Remote Broadcast omni-directional datalink, and an ultra-high frequency/very high frequency (clear or secure) voice communications package.
  - The SUW Increment integrates maritime search radar as well as Inverse Synthetic Aperture Radar and Synthetic

Aperture Radar imagery capability and the Advanced Precision Kill Weapons System (APKWS).
  - The MCM Increment is the final increment that integrates the Coastal Battlefield Reconnaissance and Analysis system and a Data Mission Payload.
- LCS components supporting the MQ-8 airframes are permanently installed on the host platform and consist of one Mission Control System (MCS), one Data Link Suite, and two Unmanned Air Vehicle Common Automatic Recovery Systems. System interoperability is achieved using the Tactical Control System (TCS) software embedded in the MCS and the host platform's command, control, communications, computers, collaboration, and intelligence architecture.

Mission

Commanders employ naval units equipped with MQ-8 airframes to provide ISR, target acquisition capability, communications relay capability, and/or APKWS in support of LCS SUW and MCM operations.

Major Contractor

Northrop Grumman – San Diego, California

Activity

- The Navy requested that USD(AT&L) certify the restructure of the Vertical Take-off and Landing Unmanned Aerial Vehicle (VTUAV) program on June 16, 2014, due to a Nunn-McCurdy breach. The Acquisition Decision Memorandum (ADM) for the restructured VTUAV program rescinded Milestone C approval for the VTUAV program granted in 2007, renamed the program as MQ-8 Fire Scout System, and designated the restructured program as an Acquisition Category (ACAT) ID Program of Record.
- Further Acquisition Category delegation to ACAT IC via the ADM occurred in June 2015. The Navy awarded a contract for 10 additional MQ-8C helicopters in September 2015 bringing the total number to 29. The Navy plans to complete their buy of the remaining 11 aircraft in FY17 prior to IOT&E. The Navy is planning to conduct the Milestone C decision for the restructured program in 2QFY17.
- COTF and VX-1 conducted the land-based QRA in response to a request by the Director, Battlespace Awareness, Operational Navy N2/N6F2, for an assessment of the operational capabilities and limitations of the radar-equipped MQ-8B to support maritime and littoral operations. The operational test events were conducted near the Naval Air Station Patuxent River over a 34-day period from May through June 2015.
- VX-1 conducted an MQ-8C OA at Naval Air Station Point Mugu, California, in November 2015 to support the upcoming Milestone C decision. This testing focused on air vehicle endurance, mission coverage, performance of the MQ-8C EO/IR sensor in a littoral environment, reliability of the system, and operator workloads.
- COTF and VX-1 conducted all operational testing in accordance with the DOT&E-approved test plans.

Assessment

- The MQ-8B QRA presented a partial assessment of radar-capable MQ-8B performance. While this QRA demonstrated the potential of the radar-capable MQ-8B, DOT&E is concerned that the land-based-only QRA presented an overly optimistic assessment of this capability. The Navy intends for the radar-equipped MQ-8B Fire Scout to launch from a host vessel capable of supporting helicopter flight operations (such as the LCS) in support of intelligence and SUW operations. This concept of operations was not demonstrated during the QRA.
- DOT&E assessed the MQ-8B performance based on QRA testing in a March 23, 2016, memorandum to the Navy, which highlighted the following results from the QRA:
  - Target location error (TLE) for radar tracks generated by MQ-8B varied from flight-to-flight. The distance to target, air vehicle speed, and whether or not the target was in the center or off-center of the radar's 180-degree search area had significant effects on TLE.
  - High flight-to-flight variability in TLE suggests that radar performance may change substantially depending on flight-specific factors that were uncontrolled in the test design, such as sea state and weather.
  - The radar-equipped MQ-8B complements the EO/IR payload capability by providing a long-range search and an all-weather target classification capability.
  - The MQ-8B radar demonstrated low detection rates for intended targets. Once potential targets were located with the radar, the MQ-8B crew demonstrated the ability to slew its EO/IR camera to the targets; determine whether these potential targets were threatening or benign; and pass information on these targets to a friendly MH-60R helicopter crew.
  - The MQ-8B demonstrated an inconsistent capability to detect target boats.
  - The MQ-8B demonstrated that the capability to employ its communications relay payload to communicate with other platforms was not consistent. During the coordinated straits transit scenario, the MH-60R and the range boats crews participating in the exercise were not able to communicate with the white cell using MQ-8B communications relay on a consistent basis.
  - During 26.3 hours of testing, testers did not observe any operational mission failures (OMFs) attributable to the AN/ZPY-4(V)1 radar.
  - MQ-8B accrued 32.3 flight hours during this QRA, experiencing two OMFs. MQ-8B suffered one OMF due to an inability to maintain a consistent Tactical Common Data Link connection, a condition known as lost link.

- Aviation vehicle operators (AVOs) and mission payload operators (MPOs) indicated that workload was generally low to moderate.
- The Radar Command and Control Station (RCCS) is a standalone laptop computer capable of displaying information from the radar including tracks generated by the Radar Subsystem (RSS), association of these tracks with AIS tracks, and information linking these tracks to known nautical features such as buoys. The MPO controls the radar via the RCCS from within the ground control station. There is no interface between the RSS and the standard MQ-8B mission payload controls.
- Operator performance demonstrated over the course of the QRA revealed gaps in training. For example, half way through the test, one MPO found that he could move the search arc of the radar when operating in short-range mode much more efficiently than the approach he had been using previously. This reduced his workload when operating the air vehicle in short-range mode.
- The Navy did not conduct cybersecurity testing during this QRA.

- The MQ-8C OA presented a partial assessment of MQ-8C performance. DOT&E is concerned that the land-based-only MQ-8C OA presented an overly optimistic assessment of this capability.
- DOT&E assessed the MQ-8C performance based on OA testing in a June 21, 2016, memorandum to the Navy, which highlighted the following results from the OA:
  - Crews employing the BRITE Star II EO/IR sensor demonstrated the ability to detect and classify targets given accurate cueing conditions. Under ideal conditions, classification ranges varied widely and did not always support sufficient stand-off distance to ensure air vehicle survivability. While these results suggest the technical performance of the sensor is meeting Navy requirements in some conditions, it is not clear whether this performance is adequate to support an LCS defense scenario.
  - Since the system's design does not tie the MQ-8C MCS directly to the ship's combat information center, there is no common operating picture between MQ-8C operators and the combat information center. MQ-8C operators must pass accurate target course and speed information to the combat information center to increase situational awareness.
  - The MQ-8C demonstrated the capability to broadcast full-motion video to ground observers equipped with a remote video terminal. The lack of trained and proficient remote video terminal operators during this OA prevents a full characterization of TAC-ISR performance.
  - The AIS is a passive receiver of commercial ship AIS broadcasts, which integrates a very high frequency transceiver with a GPS and provides identification, position, course, and speed data to the MCS over the secondary datalink. The MQ-8C system integrates the AIS into the MCS, which is a marked improvement over the MQ-8B.
  - MQ-8C operators were successful at establishing, and demonstrated the ability to relay, communications between the MCS and airspace control authorities and other land-based agencies. The sparsity of communications relay data points preludes a full characterization of communications relay capability performance. Operators did not attempt to replicate use of the communications relay capability to extend the host ship's over-the-horizon communications capability in the tactical environment.
  - The MQ-8C performance demonstrated during this OA suggests that it is on track for meeting suitability requirements at IOT&E. The data collected during the OA are not sufficient to determine if the system meets its requirements while operating as part of the LCS SUW mission package. Testing collected suitability data for MQ-8C operating from land locations.
  - The air vehicle encountered three OMFs during 82.8 flight hours for a demonstrated mean flight hours between operational mission failure rate of 27.6 hours (threshold greater than or equal to 30 hours).
  - The demonstrated operational availability exceeds the threshold requirement of 60 percent. The MQ-8C achieved the demonstrated operational availability during land-based operations.
  - The excessive presentation of nuisance Warning, Caution, and Advisory (WCAs) indications contributed to operator workload. During operator training, crews received a list of 16 nuisance WCA indications. These 16 nuisance-warning indications should alert operators to the presence of any hazardous conditions that exist. Over time, an excessive number of nuisance WCAs desensitizes operators to all WCAs. As an example, during 1 flight operators received 1,400 nuisance WCAs. During another flight, operators failed to recognize an actual WCA related to their radios. Desensitized by nuisance WCAs, operators delayed execution of the appropriate emergency procedure, and, in the event of a cascading failure, could have resulted in the air vehicle being in an unsafe situation.
  - The normal operating procedures and emergency procedures sections of the Naval Air Training and Operating Procedures Standardization (NATOPS) manual require refinement.
    - During one flight, operators following the communications relay checklist induced the loss of the command and control datalink. Once operators reestablished the datalink, developmental testers provided them with a different checklist for future use that did not induce a lost link condition.
    - During a different flight, operators encountered a failed workstation. The NATOPS procedures for this emergency induced another loss of the air vehicle command and control datalink. The loss of the command and control datalink did not become apparent until the air vehicle failed to respond to operator commands. In this case, operators called upon a developmental test engineer to reestablish the command and control datalink.

- None of the operator manuals addresses user interface menus internal to the BRITE Star II payload. Operators did not understand BRITE Star II built-in-test indications of system degradation because of this lack of documentation. In each case, mission payload operators relied upon developmental test engineers to correct the deficiency.

Recommendations

- Status of Previous Recommendations. The Navy is addressing the previous recommendations.
- FY16 Recommendations. The following recommendations are from the FY16 QRA and OA reports.
  1. Prior to fielding the radar-equipped MQ-8B in the fleet, the Navy should:
     - Consider whether an MQ-8B equipped with a 180-degree radar is capable of providing area surveillance in all operational scenarios.
     - Conduct additional testing investigating MQ-8B ability to identify intended targets during operationally realistic scenarios.
     - Identify tactics, techniques, and procedures for aircrews to maximize MQ-8B coverage of a protected entity given the inherent limitations of the radar.
     - Improve the AN/ZPY-4(V)1 radar's ability to detect targets in high clutter environments.
     - Provide an interface between the RSS and the standard MQ-8B mission payload controls so that the MPO can more easily operate the RSS and standard payload simultaneously. For example, the MPO should be able to provide the location of a track on the RSS to the AVO.
     - Characterize the performance of the AN/ZPY-4(V)1 radar in different conditions (such as high and low sea state) and in different environments so that commanders can better understand the level of accuracy and probability of detection to expect from MQ-8B system performance.
     - Provide guidelines for when crews should operate the RSS in short-range mode vice long-range mode.
     - Improve operator training by including all of the features of the RCCS, including how to cue the radar's search area efficiently while operating in short-range mode.
     - Conduct cybersecurity testing on the radar-equipped MQ-8B system.
     - Conduct additional testing to determine the maximum detection range for the AN/ZPY-4(V)1 radar-equipped MQ-8B.
  2. Prior to IOT&E and fleet introduction, the Navy should improve MQ-8C capability to assist LCS in defeating SUW attacks as an integral part of the LCS SUW mission package. Specific recommendations include:
     - Improve the center-field-of-view target course and speed algorithm to improve MQ-8C contributions to the ships common operating picture.
     - Improve BRITE Star II auto-track performance to reduce operator workload and increase tactical utility.
     - Clarify the target detection and classification ranges needed for the MQ-8C concept of operations to support LCS missions.
     - During IOT&E, conduct end-to-end HELLFIRE missile engagements to characterize the BRITE Star II auto-track capability.
     - Continue to mature the procedures checklist and emergency procedures in the NATOPS manual to allow for safe operations.
     - Eliminate nuisance WCA indications to reduce operator workload and prevent desensitization to indications.
     - Increase focus on MQ-8C emergency procedures training during operator training to allow for safe and proper operator reactions to pre-flight and in-flight anomalies.
     - Expand the MQ-8C operating theory within the training syllabus to allow operators to fully understand and react to anomalous system behavior.
     - Increase the fidelity of the MQ-8C simulator (especially BRITE Star II operations) and eliminate MQ-8B defaults to increase the value of simulator training.
     - Include instruction on the AIS and TAC-ISR payloads to operator training to allow them to properly employ and troubleshoot the systems.
     - Expand the NATOPS manual to include BRITE Star II user menus and built-in-test indications to allow operators to recognize and troubleshoot system degradations.
     - Review items required in the shipboard spare part kits to ensure inclusion of single point failure items (such as the datalink control processor) to increase system availability aboard ship.

MV-22 Osprey

Executive Summary

- The Navy conducted the first phase of Operational Test IIIK (OT-IIIK) FOT&E from March to August 2015 and a second phase of OT-IIIK from February to May 2016.
- The second phase evaluated modifications to the Defensive Weapon System (DWS) and Ramp Mounted Weapon System (RMWS) that were made after the first phase of testing.
- Modifications implemented between the first and second phase did not improve the reliability of the DWS and RMWS.
- The DWS is now compatible with the Mission Computer Obsolescence Initiative (MCOI) aircraft.

System

- The MV-22 is the Marine Corps variant of the V-22 Osprey. It is a tiltrotor aircraft capable of conventional wing-borne flight and vertical take-off and landing. The Marine Corps is replacing the now-retired CH-46 and CH-53D helicopters with the MV-22.
- The MV-22 can carry 24 combat-equipped Marines and operate from ship or shore. It can carry an external load up to 10,000 pounds over 50 nautical miles and can self-deploy 2,363 nautical miles with a single aerial refueling.
- Recent system upgrades include the following:
  - MCOI. The MCOI computer hardware initiative is designed to improve the performance of the existing Advanced Mission Computer architecture by adding greater processing speed and more data storage while maintaining the same functionality as the original computer.
  - Blue Force Tracker 2 (BFT-2). The updated BFT-2 GPS-enabled system receives information on friendly, neutral, and hostile forces, as well as sends and receives text and image messages via a federated cockpit display.
  - DWS. GAU-17 DWS improvements add a sensor-only mode that allows the gunner to use the electro-optical sensor when the gun turret is not being used. The turreted, remotely operated, all-quadrant, 7.62 mm DWS is designed for fire suppression against ground troops and soft targets.
  - RMWS. The GAU-21 .50 caliber RMWS replaced the GAU-18 RMWS.

Mission

- Squadrons equipped with MV-22s provide medium-lift assault support in the following operations:
  - Ship-to-Objective Maneuver
  - Sustained operations ashore
  - Tactical recovery of aircraft and personnel
  - Self-deployment
  - Amphibious evacuation

Major Contractors

Bell-Boeing Joint Venture:

- Bell Helicopter – Amarillo, Texas
- The Boeing Company – Ridley Township, Pennsylvania

Activity

- Testing activity focused on the four recent upgrades to the MV-22. The first phase of OT-IIIK was conducted from March to August 2015. The Navy conducted a second phase of OT-IIIK FOT&E from February to May 2016, which evaluated modifications designed to address deficiencies in the DWS and to the RMWS that were discovered in the first phrase of testing. Testing was done in accordance with the DOT&E-approved test plan.
- Marine Corps pilots conducted testing at locations with conditions representative of those encountered in fleet operations. These locations included Marine Corps Base Camp Lejeune, North Carolina; at or near Kirtland AFB, New Mexico; and at or near Marine Corps Air Station Yuma, Arizona. They used three production-representative Advanced Mission Computer aircraft and a production-representative MCOI aircraft. The Advanced Mission Computer configuration is the original, pre-MCOI configuration.
- The Navy's Commander, Operational Test and Evaluation Force, with assistance from Marine Operational Test and Evaluation Squadron 22, conducted cybersecurity testing of

the MV-22 aircraft, mission planning system, and maintenance systems from May 4 – 8, 2015, at Marine Corps Air Station New River, North Carolina. The cybersecurity evaluation was based upon an Adversarial Assessment that included a test of the ability of the unit to protect against cyber-attacks, detect and respond to a cyber-attack, and restore to normal operations in the event of a successful cyber-attack. At the current time, the Navy does not have the capability to do cybersecurity testing on Military Standard (MIL-STD)-1552 data buses, so those were not evaluated.

Assessment

- The upgrades did not enhance the operational effectiveness, suitability, or survivability of the MV-22-equipped unit and MV-22 units remain effective, suitable, and survivable.
- Crews employing MV-22 aircraft equipped with updated mission computers (commonly referred to as "MCOI-equipped") discovered two deficiencies that would hinder the ability of a MCOI-equipped unit to perform its mission:
  1. Pilots reported that numbers and text on the cockpit displays in the MCOI aircraft were not as sharp as those in legacy aircraft despite the new displays' higher resolution.
  2. The MCOI hover display mode did not transition into and out of hover mode without extra pilot actions.
- MCOI aircraft demonstrated compatibility with the DWS in Phase 2, which was not the case in Phase 1.
- The BFT-2 delivery of digital messages is improved over BFT-1. BFT-2 pilot workload remains high for use in a busy cockpit. The BFT 2 transfer of digital images did not work.
- Inherent deficiencies in the design of the DWS continue to limit the unit's ability to provide suppressive fire against threat targets. The Phase 2 modifications to the DWS design had no measureable effect on the aircrew's capability to provide suppressive fire with the DWS.
- The field of fire of the RMWS has expanded and the gun provides suppressive fire to the rear when it fires, but the RMWS cannot be counted on to fire when needed.
- Modifications to the DWS and RMWS did not improve the effectiveness or reliability of the weapon systems.
- After conclusion of the 2016 test period, fuselage damage to several test aircraft was discovered in an area not usually inspected during normal postflight procedures. This damage was discovered in the vicinity of where the DWS ejects shell casings.
- During testing, the OT-IIIK MV-22 aircraft met reliability requirements but did not meet maintainability and availability thresholds. Demonstrated reliability, maintainability, and availability performance is consistent with that of the MV-22 fleet.
- Cybersecurity vulnerabilities were discovered during testing; the details of which are classified.
- The Air Force Special Operations Command observed repeated problems with the CV-22 Icing Protection System (IPS) during testing of the Tactical Software Suite this year, as stated in the CV-22 Annual Report. As the MV-22 has the same system, there could be similar problems on its system.

Recommendations

- Status of Previous Recommendations. The Navy has not completed actions to address the following FY15 recommendations:
  - Address failure modes and supply issues that limit aircraft availability.
  - Use Marine Air-Ground Task Forces to employ tactics, techniques, and procedures to compensate for limitations in the DWS.
  - Improve BFT-2 message latency.
  - Investigate and improve RMWS reliability.
  - Address cyber vulnerabilities of the MV-22 and its supporting systems.
- FY16 Recommendations. The Navy should:
  1. Continue to execute a viable reliability growth program for the MV-22 fleet, and address failure modes that degrade aircraft availability.
  2. Address the MCOI shortcomings and focus on improving the clarity of cockpit displays and modifying the hover page function so that it always returns to the previously selected page.
  3. Investigate and remedy the cause of BFT-2 image messaging failures.
  4. Continue to investigate and remedy the causes of reliability failures in the DWS and RMWS.
  5. Inspect the MV-22 fleet for possible fuselage damage caused by the DWS. If damage is discovered, the cause should be investigated and prevention/remediation actions should be taken.
  6. Address cybersecurity vulnerabilities of the MV-22 and supporting systems.
     a. Develop the capability to conduct cybersecurity testing of MIL-STD-1553 data buses.
     b. Investigate whether modifications to aircraft restore procedures are needed after a cyber-attack.
  7. Investigate MV-22 IPS performance fleet-wide. If MV-22 IPS problems are discovered, the Navy should initiate improvement actions to correct repeated IPS failures.

Next Generation Jammer (NGJ) Increment 1

Executive Summary

- The USD(AT&L) signed an Acquisition Decision Memorandum (ADM) on April 5, 2016, approving Milestone B and entry into the Engineering and Manufacturing Development (EMD) phase for the Next Generation Jammer (NGJ) Increment (Inc) 1 program.
- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted an Early Operational Assessment (EOA) between June, and October 2015, to assess the current status of the NGJ Inc 1 technical design, examine the NGJ Inc 1 potential capabilities to satisfy future EA-18G Airborne Electronic Attack (AEA) mission requirements, and identify any risks to successful completion of the IOT&E in FY21.
- DOT&E submitted an EOA report on February 10, 2016, in support of the Milestone B decision. The EOA was a preliminary assessment and thus did not present conclusions on NGJ Inc 1 operational effectiveness, suitability, or survivability. The EOA did assess the potential strengths and weaknesses of the NGJ Inc 1 design, effects on the EA-18G aircraft while carrying the NGJ Inc 1, and potential limitations to the successful completion of IOT&E.
- Given the current state of the test ranges, the NGJ Inc 1 testing was adequate, albeit with substantial limitations. However, with the DOT&E-recommended DOD Enterprise-wide range improvements, which will serve numerous acquisition systems for testing, the upgraded ranges will enable both adequate open air testing and validation of modeling and simulation against operationally relevant threats during the NGJ Inc 1 IOT&E.
  - The improved ranges will require numerous programs, to include NGJ Inc 1, to revisit their respective evaluation frameworks.
  - The electronic warfare range upgrades that DOT&E has identified and recommended for funding to the Department's Leadership are needed to conduct adequate testing of NGJ and other key systems without the substantial degradations in operational realism limitations that current test capabilities impose.

System

- The NGJ system is a replacement for the ALQ-99 Tactical Jamming System pods that were initially developed and fielded in 1971 on the EA-6B aircraft to perform AEA against radars associated with threat integrated air defense systems. The ALQ-99 pods have been flown more recently on the EA-18G aircraft that entered full-rate production in FY09.
- The NGJ system is an evolutionary acquisition program designed to provide capability in three increments: Inc 1 (Mid-Band), Inc 2 (Low-Band), and Inc 3 (High-Band). The order of development was determined by the assessed capabilities of the developing threat and shortfalls of the legacy system to counter those capabilities, with Inc 1 covering the most critical threats. Inc 1 was the only increment in development during FY16.
- NGJ Inc 1 will be deployed as an AEA system on the EA-18G aircraft, working with the organic ALQ-218 receiver system and off-board assets as a component of future carrier air wings and expeditionary forces, providing capabilities against a wide variety of radio frequency targets. NGJ Inc 1 is intended to expand the current ALQ-99 mission set to include non-kinetic attack against a full spectrum of agile and adaptive communications, datalinks, and non-traditional radio frequency targets.

Mission

- Commanders will use the NGJ Inc 1 to deny, degrade, or deceive the enemy's use of the electromagnetic spectrum employing both reactive and pre-emptive jamming techniques, while enhancing the friendly force's use of the electromagnetic spectrum.
- AEA increases the survivability of joint forces tasked to enter denied battlespace and engage anti-access threats/high-value targets and provides additional means via Information Operations to thwart enemy offensive actions.

Major Contractors

- Raytheon Space and Airborne Systems – El Segundo, California
- The Boeing Company, Defense, Space & Security – St. Louis, Missouri

Activity

- The USD(AT&L) signed an ADM on April 5, 2016, approving Milestone B and entry into the EMD phase. The ADM also:
  - Designated the NGJ Inc 1 program as an Acquisition Category ID Major Defense Acquisition Program
  - Authorized the Navy to proceed with the award of the EMD contract, which includes a future modification for four System Demonstration Test Article ship-sets (two pods per ship-set) and support to operational testing
  - Authorized a low-rate initial production quantity of up to 30 ship-sets
- An EOA was conducted by COTF between June and October 2015, in accordance with the DOT&E-approved Test and Evaluation Master Plan and test plan. The EOA was conducted to assess the current status of the technical design, to examine potential capabilities to satisfy future EA-18G AEA mission requirements, and to identify any risks to successful completion of the IOT&E in FY21. DOT&E submitted an EOA report on February 10, 2016, in support of the Milestone B decision.
- An operational assessment is scheduled for 3QFY19.

Assessment

- The EOA was a preliminary assessment and thus did not present conclusions on NGJ Inc 1 operational effectiveness, suitability, or survivability.
- Potential strengths of the NGJ Inc 1 design demonstrated during the EOA were:
  - High Effective Isotropic Radiated Power (EIRP) for larger stand-off ranges
  - Wide frequency range to counter more frequency diverse threats
  - Large field of regard for operations in a dense threat environment
  - Sufficient Ram-air Turbine Generator power generation to provide the pod system with the power required without drawing from the host platform
- Potential weaknesses of the NGJ Inc 1 design demonstrated during the EOA were:
  - Degraded ALQ-218 host platform receiver capability due to radio frequency interoperability problems caused by higher EIRP requirements
  - Hazards of Electromagnetic Radiation to Ordnance effects on the AGM-88 High-speed Anti-Radiation Missile/ Advanced Anti-Radiation Guided Missile affecting reliability
- Based on early small-scale wind tunnel testing and current computational fluid dynamics (CFD) modeling, there is decreased margin to meeting the EA-18G mission radius.
- COTF identified potential limitations to the successful completion of IOT&E through visits to modeling and simulation (M&S) facilities and focus groups with test resource staff, test engineers, test aircrew, and operational stakeholders. The currently-approved M&S plan sufficiently covers M&S for EMD. This plan will need to be updated prior to Milestone C to incorporate specific IOT&E requirements. Additionally, scheduling of the test ranges, test aircraft, test aircrew, and maintenance personnel needs to be planned for well in advance of the beginning of IOT&E due to limitations in availability and conflicting EA-18G test programs.
- Given the current state of the test ranges, the NGJ Inc 1 testing was adequate, albeit with substantial limitations. However, with the DOT&E-recommended DOD Enterprise-wide range improvements, which will serve numerous acquisition systems for testing, the upgraded ranges will enable both adequate open air testing and validation of modeling and simulation against operationally relevant threats during the NGJ Inc 1 IOT&E.
  - The improved ranges will require numerous programs, to include NGJ Inc 1, to revisit their respective evaluation frameworks.
  - The electronic warfare range upgrades that DOT&E has identified and recommended for funding to the Department's Leadership are needed to conduct adequate testing of NGJ and other key systems without the substantial degradations in operational realism limitations that current test capabilities impose.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Navy should:
  1. Perform planned wind tunnel and CFD modeling of the NGJ Inc 1 configuration as it matures during EMD to predict installed aircraft performance.
  2. Perform planned testing and analysis to determine the extent of Hazards of Electromagnetic Radiation to Ordnance effects on operational use of the AGM-88 High-speed Anti-Radiation Missile/Advanced Anti-Radiation Guided Missile.
  3. Update the M&S plan prior to Milestone C to incorporate specific IOT&E requirements.
  4. Prioritize resources to ensure the test ranges, test aircraft, test aircrew, and maintenance personnel needed to execute IOT&E are available when required.
  5. Fund range upgrades and have all programs, to include NGJ Inc 1, test against the improved ranges.

P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)

Executive Summary

- In FY16, the Navy completed the P-8A Data Storage Architecture Upgrade (DSAU)/Verification of Correction of Deficiencies (VCD) FOT&E. DOT&E's May 2016 P-8A DSAU/VCD operational test report concluded that the DSAU modification provided an effective data transfer and storage architecture to replace legacy system components. The modification effectively reduced the number of data transfer and media recording devices without introducing new system deficiencies. The associated Fleet Release 35 operational flight software successfully corrected seven previously identified system deficiencies. These corrections provided marginal improvements to system performance and user interfaces that affect the mission areas of anti-submarine warfare (ASW); intelligence, surveillance, and reconnaissance (ISR); and aircraft mobility.
- The Navy delayed the P-8A Engineering Change Proposal (ECP) 2 OT&E, originally planned for early FY16, until 1QFY17 due to developmental ASW software deficiencies. This operational test period includes: re-evaluation of the P-8A wide-area ASW search capability with the Multi-static Active Coherent (MAC) Phase I sensor system; complete re-evaluation of the P 8A ISR mission, including both imagery and signals intelligence capabilities; evaluation of air-to-air refueling; cybersecurity assessment; and evaluation of additional AGM-84 Harpoon employment modes. Operational testers will also collect reliability, maintainability, and availability data during this test period to re evaluate P-8A fleet operational availability with a fully mature logistics support system in place. The ECP 2 OT&E will be the most extensive P-8A operational test conducted since the 2012 P-8A IOT&E.
- The Navy continues to delay the development of the MAC system and MAC tactics for deep water and convergence zone acoustic environments. Thus, even after fielding ECP-2, the P-8A will not have an effective wide area acoustic ASW search capability in many threat ocean areas.
- In April 2016, USD(AT&L) approved a revised Navy P-8A acquisition strategy which incorporated all P-8A Increment 3 capability requirements into the baseline P-8A program. These capabilities will now be developed and delivered as a series of ECPs designated as ECPs 4 through 7. They include implementation of significant open system architecture changes, ASW capability enhancements, communication system upgrades, radar and electronic signal sensor upgrades, and AGM-84 Harpoon 2+ anti-ship missile integration. Navy development of a comprehensive Test and Evaluation Master Plan (TEMP) and test schedule for the new P-8A ECP capability releases has been delayed due to evolving capability requirements, potential budget reductions, and schedule uncertainties. TEMP development activities are currently behind schedule to support the start of ECP 4 testing in 2QFY17.

System

- The P-8A Poseidon Multi-mission Maritime Aircraft (MMA) design is based on the Boeing 737-800 aircraft with significant modifications to support Navy maritime patrol mission requirements. It is replacing the P-3C Orion.
- The P-8A incorporates an integrated sensor suite that includes radar, electro-optical, and electronic signal detection sensors to detect, identify, locate, and track surface targets. An integrated acoustic sonobuoy launch and monitoring system detects, identifies, locates, and tracks submarine targets. Sensor systems also provide tactical situational awareness information for dissemination to fleet forces and ISR information for exploitation by the joint intelligence community.
- The P-8A carries MK 54 torpedoes and the AGM-84D Block 1C Harpoon anti-ship missile system to engage submarine and maritime surface targets.
- The P-8A aircraft incorporates aircraft survivability enhancement and vulnerability reduction systems. An integrated infrared missile detection system, flare dispenser, and directed infrared countermeasure system is designed to improve survivability against infrared missile threats. On and off-board sensors and datalink systems are used to improve tactical situational awareness of expected threat systems. Fuel tank inerting and fire protection systems reduce aircraft vulnerability.
- The Navy is integrating the MAC sensor system into the P-8A to provide a wide-area, active ASW search capability.
- Planned future upgrades include the addition of the High Altitude ASW Weapon Capability (HAAWC), AGM 84 Harpoon II+, MAC wide-area ASW search enhancements,

signals intelligence sensors, and advanced mission system architectures and processing upgrades.

Mission

- Theater Commanders primarily use units equipped with the P-8A MMA to conduct ASW operations including the detection, identification, tracking, and destruction of submarine targets.
- Additional P-8A maritime patrol missions include:
  - ASW operations to detect, identify, track, and destroy enemy surface combatants or other maritime targets
  - ISR operations to collect and disseminate imagery and signals information for exploitation by the joint intelligence community
  - Command, control, and communication operations to collect and disseminate tactical situation information to fleet forces
  - Identification and precise geolocation of targets ashore to support fleet strike warfare missions

Major Contractor

Boeing Defense, Space, and Security – St. Louis, Missouri

Activity

- In FY16, the Navy completed the P-8A DSAU/VCD FOT&E. This test evaluated improvements in ASW and ISR mission data loading and storage following the DSAU modification. This test event also included testing to verify corrections for nine previously identified weapons bay, electronic signal collection, Information Assurance, and avionics integration deficiencies, as well as a system-level cybersecurity assessment. DOT&E released the P-8A DSAU Operational Test Report in May 2016.
- The Navy developed improvements to the P-8A acoustic system, the Active System Performance Estimate Computer Tool, and the MAC program that were designed to improve ASW capability. The Navy updated MAC search tactics in shallow water environmental areas and continues to develop the tactics and MAC system upgrades for deeper ocean areas.
- The Navy delayed the P-8A ECP 2 OT&E, originally planned for early FY16, until 1QFY17 due to developmental ASW software deficiencies. This test will evaluate P-8A wide-area ASW search capability with the MAC Phase I sensor system; P-8A ISR capabilities, including both imagery and signals intelligence collection; air-to-air refueling; cybersecurity; and additional AGM-84D Block 1 Harpoon missile employment modes. Operational testers will also collect reliability, maintainability, and availability data during this test period to re-evaluate P-8A fleet operational availability with a fully mature logistics support system in place.
- Contractor and government developmental testing of HAAWC system capability to employ sonobuoys and the MK 54 torpedo from the P-8A at medium to high altitudes is in progress. As a result of increased program cost estimates and reduced funding, the Navy transferred resource sponsor organizational responsibilities within the Navy staff and is currently revising performance thresholds in the HAAWC draft Capabilities Development Document. The HAAWC program has not yet developed a comprehensive test strategy and does not have an approved TEMP.
- In April 2016, USD(AT&L) approved a revised Navy P-8A acquisition strategy which incorporated all P-8A Increment 3 capability requirements into the baseline P-8A program. These capabilities will now be developed and delivered as a series of ECPs designated as ECPs 4 through 7. They include implementation of significant open system architecture changes, ASW capability enhancements, communication system upgrades, radar and electronic signal sensor upgrades, and AGM-84 Harpoon 2+ anti-ship missile integration. The Navy is currently working to develop a revised P-8A TEMP to define the developmental and operational test strategy for this new series of ECPs. Per the approved P-8A acquisition strategy, the Navy should submit a revised P 8A TEMP for DOT&E approval prior to the start of ECP 4 testing in 2QFY17. Tentative test schedules include a series of ECP operational test events in FY18, FY19, FY21, and FY22 to support the incremental release of new P-8A capabilities.
- The Navy completed the second lifetime of fatigue and durability testing on P-8A full-scale test aircraft in FY15 and conducted extended lifetime testing in FY16. Teardown and final analysis of the full-scale fatigue test aircraft will occur when the extended life testing is completed in FY17. Residual strength testing on both the full-scale test article and horizontal stabilizer was also completed in FY16. Main and nose landing gear subassemblies completed the equivalent of three lifetimes of fatigue testing in FY15, followed by landing gear post-test teardown and analysis in FY16.

Assessment

- DOT&E's May 2016 P-8A DSAU/VCD operational test report concluded that the DSAU modification provided an effective data transfer and storage architecture to replace legacy system components. The modification effectively reduced the number of data transfer and media recording devices without introducing new system deficiencies. The associated Fleet Release 35 operational flight software successfully corrected seven previously identified system deficiencies and partially corrected one additional deficiency. These corrections provide marginal improvements to system performance and user interfaces that affect ASW, ISR, and aircraft mobility mission areas. These improvements do not significantly alter previous assessments of overall P-8A mission capabilities.
- The P-8A DSAU/VCD FOT&E cybersecurity test events identified a collection of exploitable P-8A cybersecurity

vulnerabilities. Based on the results of this test, DOT&E recommended that the Navy conduct a more comprehensive P-8A cybersecurity test to include end-to-end cyber-attack and response threads for the complete P-8A system-of-systems, including maintenance support systems, Tactical Mobile mission planning and support systems, and physical access points to P-8A integrated workstations. The Navy is planning to include an expanded cybersecurity test event as part of the FY17 P-8A ECP 2 OT&E.

- The Navy's FY17 P-8A ECP 2 OT&E evaluates significant new P-8A capabilities, including wide-area ASW search with the MAC Phase I sensor system, air-to-air refueling, and additional AGM-84 Harpoon employment modes. It also includes a complete re-evaluation of P-8A imagery and signals intelligence collection capabilities. This will be the most extensive P 8A operational test conducted since the 2012 P-8A IOT&E.
  - The Navy did not complete the development of MAC capability or MAC tactics for wide-area active ASW search in deep or Convergence Zone acoustic environments; therefore, the P-8A ECP-2 OT&E will only evaluate improvements to the MAC Phase I system in shallow and littoral environments. Thus, the P-8A does not have the full wide-area acoustic ASW capability required by the baseline Capability Development Document.
  - The Navy continues to develop and test corrective actions for 106 open system deficiencies identified as operationally significant during previous test periods. The ECP 2 OT&E test plan includes events to verify corrective actions for 37 of these deficiencies. During this test, operational testers will also collect reliability, maintainability, and availability data during this test period to re-evaluate P 8A fleet operational availability with a fully mature logistics support system in place.
- The Navy continued ECP-2 testing to evaluate improvements to the P-8A's acoustic and MAC software and employment tactics in representative littoral shallow water environments. The Navy continues to develop tactics and system improvements to use the MAC system in deeper water ASW environments. A higher source level active buoy is undergoing developmental testing; when combined with new tactics and MAC software improvements, it could improve and expand the current ECP-2 ASW capability. Once the new MAC source buoy is completed and fielded, a re-evaluation of the MAC capability will be required. This testing will be included in the updated P-8A TEMP.
- The Navy's contractor testing of the HAAWC MK 54 weapon delivery capability is progressing. The contractor completed two successful test flights in FY16. The P-8A program conducted initial testing to verify the HAAWC captive carriage, buffet load margins, and safe separation.
- The Navy delayed development of a comprehensive test strategy and schedule for the new P-8A ECPs 4 through 7 (formerly the P-8A Increment 3 program) due to evolving capability requirements, potential budget reductions, and schedule uncertainties. Development of a revised P-8A TEMP is necessary to ensure that test resources are defined and available to support development of P-8A open system architecture changes, enhanced ASW capabilities, communication system upgrades, radar and electronic signal sensor upgrades, and AGM-84 Harpoon 2+ anti-ship missile integration. Navy TEMP development activities are currently behind schedule to support the start of ECP 4 testing in 2QFY17.
- The Navy completed landing gear fatigue test assembly data analysis with no significant findings. Teardown of the full-scale aircraft fatigue test article will occur when all extended life test events are complete. The program continues to review the full-scale test article data to refine fleet airframe inspection requirements and depot repair procedures to ensure the airframe meets the intended 25-year design life. To date, no significant long term structural problems have been identified.

Recommendations

- Status of Previous Recommendations. The Navy made progress on all three FY15 recommendations. The Navy completed P-8A ECP 1 OT&E to evaluate initial P-8A MAC wide-area search capabilities. The program also initiated TEMP development for the new P-8A ECPs 4 through 7 capability enhancements (formerly P-8A Increment 3). The Navy also verified correction of 7 previously identified system deficiencies in FY16 and planned verification of an additional 37 (of 106 remaining) system deficiencies in FY17.
- FY16 Recommendations. The Navy should:
  1. Submit a comprehensive P-8A TEMP for DOT&E approval covering new P-8A ECPs 4 through 7 and MAC system improvements prior to the start of ECP 4 testing in FY17.
  2. Continue to implement corrective actions for the significant number of operationally significant system deficiencies identified in previous P-8A operational test reports and conduct additional follow-on operational tests to verify improved mission capabilities.
  3. Conduct a comprehensive P-8A cybersecurity evaluation to include complete end-to-end cyber-attack and response threads for the P-8A aircraft and key mission support systems.

Remote Minehunting System (RMS)

Executive Summary

- In the wake of the Navy's 2015 Technical Evaluation (TECHEVAL) of the Increment 1 mine countermeasures (MCM) mission package, and following the Navy's independent review of the program, the Navy cancelled the Remote Minehunting System (RMS) program and announced its intention to evaluate alternatives to the RMS. Those alternatives included use of an unmanned surface vessel (USV) to tow improved minehunting sensors and the Knifefish unmanned undersea vehicle (UUV). The Navy's decision came after approximately two decades of RMS development and repeated claims by Navy officials that the system had achieved remarkable reliability growth in recent years. As illustrated clearly in the FY15 edition of this report, the Navy's claims regarding reliability improvement were demonstrably incorrect.
- The Navy has reportedly funded refurbishment of a small number of the existing Remote Multi-Mission Vehicles (RMMVs) and may still employ these vehicles in some capacity. However, planning for developmental and operational testing of the mission package is proceeding under the assumption that the future minehunting capability will be provided by one or two USVs towing an AN/AQS-20C or AN/AQS-24C minehunting sensor and a pair of Knifefish UUVs.
- The Navy continued to develop pre-planned product improvements for the AN/AQS-20 sonar in FY16. It's plans to commence realistic AN/AQS-20C developmental and operational testing are uncertain because of limited availability of two potential tow platforms; existing RMMVs are not reliable but the Navy does not expect to begin upgrades necessary to make the initial, limited-quantity USVs compatible with the improved sonar until at least FY18.

System

- The RMS is designed to provide off-board mine reconnaissance capability to detect, classify, and localize non-buried bottom and moored mines, and to identify bottom mines in shallow water.
- RMS uses the RMMV, which is an unmanned, diesel-powered, semi-submersible vehicle, to tow the AN/AQS-20 variable depth sensor.
  - The AN/AQS-20 is a multi-mode sensor in a modular towed body that can house as many as five sonars. The AN/AQS-20 can also be fitted with an electro-optical identification device to identify mine-like objects. The Navy is developing a new variant of the sensor, designated AN/AQS-20C, which includes an improved forward-looking sonar and new synthetic aperture side-looking sonars. The Navy expects to field the AN/AQS-20C by FY18 or FY19, pending availability of a tow vehicle.

  - Although the Navy cancelled the RMS program and suspended further RMMV procurement, it plans to overhaul some of the existing RMMVs for possible deployment with early variants of the Littoral Combat Ship (LCS) MCM mission package. The Navy is also developing the capability to tow a minehunting sensor (AN/AQS-20C or AN/AQS-24) with an USV (based on the vessel used in the Unmanned Influence Sweep System being developed for LCS) to replace the RMS.
- A datalink subsystem provides real-time communications between the host ship and the RMMV for command and control and transmission of some sensor data. The RMS datalink subsystem, which includes ultra-high frequency line-of-sight (LOS) and low-band very-high frequency over-the-horizon (OTH) radios, interfaces with the multi-vehicle communications system installed in the LCS seaframes.
- Shipboard operators control the RMMV using a remote minehunting functional segment integrated into the LCS mission package computing environment.
- The RMS records sensor data to a removable hard drive during minehunting operations. Following vehicle recovery, operators transfer data to an organic post mission analysis station and review sonar data to mark contacts as suspected mine-like objects. The RMS does not determine the absence or presence of mines or complete mine clearance operations in a single pass. Following an initial search by the RMS, sailors plan additional RMS sorties in the same area to assess persistence of in-volume contacts marked as mine-like and to identify bottom contacts marked as mine-like as either mines or non-mines. When operators conclude that RMS in-volume contacts are persistent, those contacts are passed to another system for identification and neutralization.

Mission

If the system is fielded, MCM Commanders would likely employ the RMS from an MCM mission package-equipped LCS, to detect, classify, and localize non-buried bottom and moored mines, and to identify shallow-water bottom mines in support of theater minehunting operations.

Major Contractors

- RMMV: Lockheed Martin – West Palm Beach, Florida
- AN/AQS-20 (all variants): Raytheon Corporation – Portsmouth, Rhode Island

---

Activity

- The Navy initiated RMS cybersecurity testing and conducted additional ship-based RMS testing to assess readiness for operational testing that it expected to complete in FY15
- In October 2015, the Navy delayed IOT&E of the *Independence*-variant LCS equipped with the first increment of the MCM mission package pending the outcome of an independent program review, including an evaluation of potential alternatives to the RMS. The Navy chartered the review in response to an August 21, 2015, letter from Senators John McCain and Jack Reed, Chairman and Ranking Member of the Senate Committee on Armed Forces expressing concerns about the readiness to enter operational testing given the significant reliability problems observed during a TECHEVAL in 2015.
- In early 2016, following the completion of the independent review, the Navy:
  - Concluded that reliance on shore-based test metrics provided a false sense of RMMV maturity and contributed to the RMS progressing to sea-based test events prematurely.
  - Cancelled the RMS program and halted further RMMV procurement.
  - Announced its intention to field existing RMMVs following overhauls to mitigate high impact failure modes.
  - Revealed initial plans (subsequently dashed by lack of funding for Knifefish improvements) to evaluate alternatives to the RMS, including an USV towing either the AN/AQS-20C or AN/AQS-24C minehunting sensor and an improved version of the Knifefish UUV already in development.
  - Abandoned plans to conduct operational testing of individual MCM mission package increments and delayed the start of LCS MCM mission package IOT&E until at least FY20.
- In June 2016, DOT&E submitted an early fielding report to the Congress in response to the Navy's plan to deploy the *Independence*-variant LCS equipped with the MCM mission package, including the existing v6.0 RMMVs and AN/AQS-20As, prior to the conduct of operational testing. The classified report, which does not support the Full-Rate Production decision, provided DOT&E's interim assessments of operational effectiveness and operational suitability of the *Independence*-variant LCS employing the MCM mission package and its components, including the RMS.
- The Navy continued to develop pre-planned product improvements for the AN/AQS-20 sonar in FY16. It's plans to commence realistic AN/AQS-20C developmental and operational testing are unsettled because of limited availability of two potential tow platforms; existing RMMVs are not reliable but the Navy does not expect to make the initial, limited-quantity USVs compatible with the AN/AQS-20C until late FY18. In testimony to the Senate Armed Services Committee in December, the Navy announced that two RMMVs will be groomed and one will be overhauled. These RMMVs will then be used to continue AN/AQS-20 sonar testing, conduct data collection, and support user evaluation until the first USV is available.

Assessment

- The RMS would not be operationally effective or operationally suitable if called upon to conduct MCM missions in combat. The primary reasons for these conclusions are:
  - The system is not reliable.
  - The system's minehunting capabilities are limited in other-than-benign environmental conditions.
  - The fleet is not equipped to maintain the system.
- Since the Navy has not implemented corrective actions to mitigate the problems observed in earlier testing, the substantive unclassified details of DOT&E's assessment are unchanged from the FY15 edition of this report. DOT&E's classified June 2016 early fielding report provides additional detail.

Recommendations

- Status of Previous Recommendations.
  - The Navy made progress on all four FY13 recommendations. Shore-based testing completed in 1QFY14 and shipboard testing completed in 1QFY15 provided additional information regarding RMS, RMMV, and AN/AQS-20A reliability; RMS operational availability; and RMMV launch, handling, and recovery system performance. Although the Navy continues to develop and test AN/AQS-20 upgrades, it has not demonstrated in developmental or operational testing that it has corrected problems with false classifications and contact localization errors that will otherwise limit performance in operational testing. The Navy has not determined the test program for the AN/AQS-20 sonar yet, but will include that as an annex to the LCS TEMP rather than having a separate document.
  - The Navy has made progress on two of the nine FY14 recommendations. The Navy did not act on the following FY14 recommendations:

- Conduct testing of the RMS consisting of the v6.0 RMMV and AN/AQS-20B/C in operationally realistic end-to-end minehunting missions to characterize minehunting performance and accurately assess availability of the RMS and reliability of the RMMV and sonar.
- Investigate the use of communications relays and other solutions that might improve the standoff distance between an RMMV and its host ship to improve the efficiency of LCS MCM operations.
- Reassess RMMV v6.0 radiated noise following vehicle upgrades.
- Reexamine minimum vehicle and sensor reliability and LCS organizational-level maintenance support needed to complete timely and realistic operational scenarios without excessive reliance on intermediate- and depot-level support.
- Reconsider RMS minehunting requirements in the context of expected LCS tactics and operations.

- By reviewing alternatives to the RMMV, the Navy has made progress on one of the six FY15 recommendations. The Navy did not act on the following FY15 recommendations, which are applicable to RMS and potential replacement systems:
  - Complete a comprehensive review of RMMV and mission package communications interfaces and, if necessary, re-engineer the Multi-Vehicle Communication System (MVCS), RMMV, and/or other essential system-of-systems components to improve interoperability and enable reliable line-of-sight and over-the-horizon communications between LCS and RMMVs.
  - Develop tactics to mitigate system vulnerabilities to mines and other hazards.
  - Assess improvements to post mission analysis and contact management software and training to resolve problems observed during TECHEVAL when multiple RMS contacts on the same mine were passed to AMNS for identification and neutralization.
  - Continue to develop and implement improvements for launch, handling, and recovery equipment and procedures.
  - Provide LCS sailors better training, technical documentation, test equipment, and tools, along with additional spares to improve the crews' self-sufficiency and enhance RMS maintainability.

- FY16 Recommendations. The Navy should address the prior applicable recommendations and consider the following actions:
  1. Suspend further use of RMMV v6.0 until completing a comprehensive reliability-centered analysis, correcting high impact failure modes, and testing repairs in an operationally realistic environment.
  2. Complete a comprehensive LCS-based cybersecurity assessment of the RMMV before deploying any existing units for operational use.
  3. Limit procurement of AN/AQS-20 sonars and upgrade kits, which are not yet meeting the Navy's original requirements and negatively affect LCS MCM capability, until much needed performance improvements are developed, tested, and proven effective in testing representative of realistic LCS mine-clearance operations.
  4. Given the cancellation of the RMS program, fully fund and accelerate the development of the most promising minehunting alternatives, including the USV with a towed AN/AQS-20C or AN/AQS-24C sensor and the Knifefish UUV with pre-planned product improvements.

Rolling Airframe Missile (RAM) Block 2

Executive Summary

- DOT&E issued a classified Early Fielding Report to Congress on March 23, 2016, because a ship deployed with the Rolling Airframe Missile (RAM) Block 2 system prior to completion of IOT&E. Based on all the results of the completed IOT&E tests, DOT&E stated that:
  - Insufficient data exist to characterize RAM Block 2's performance against all the anti-ship cruise missile (ASCM) threats the missile is intended to defeat. This condition will continue until the Navy completes RAM Block 2 IOT&E, which is expected in late 2017.
  - Completed testing has demonstrated that RAM Block 2 incorporates several improvements over its RAM Block 1 and 1A predecessors.
  - Deficiencies in RAM Block 2 integration with the Ship Self-Defense System (SSDS)-based combat system caused several RAM Block 2 missiles to miss their target during one of the IOT&E missile firing scenarios.
  - Due to the Navy's inability to develop a Multi-Stage Supersonic Target (MSST), no assessment of RAM Block 2's capability against MSST-like ASCM threats is possible.
  - RAM Block 2 met its in-flight reliability requirement.
- The Navy's Commander, Operational Test and Evaluation Force (COTF) continued the IOT&E with one RAM Block 2 missile firing scenario at the Naval Air Warfare Center, Point Mugu, California, in April 2016 from the Self-Defense Test Ship in accordance with a DOTE-approved test plan.

System

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat ASCMs. There are three RAM variants:
  - RAM Block 0 uses dual mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defenses against ASCMs that do not radiate radio frequencies.

  - RAM Block 2 incorporates changes to improve its kinematic capability and capability to guide on certain types of ASCM radio frequency threat emitters in order to defeat newer classes of ASCM threats.
- RAM Block 2 can be launched from the 21 round RAM Guided Missile Launch System resident on LPD 17, LHA 6, LSD 41/49, LCS *Freedom*, and CVN 68 ship classes or from the SeaRAM standalone self-defense system composed of the Close-In Weapon System radar/electronic warfare sensor suite and command/decision capability combined with an 11-round missile launcher which is resident on selected Aegis DDG 51 Destroyers and the LCS *Independence* ship class.

Mission

Commanders employ naval surface forces equipped with RAM to provide a defensive short-range, hard-kill engagement capability against ASCM threats.

Major Contractors

- Raytheon Missiles Systems – Tucson, Arizona
- RAMSys – Ottobrunn, Germany

Activity

- DOT&E issued a classified Early Fielding Report to Congress on March 23, 2016, because a ship deployed with the RAM Block 2 system prior to completion of IOT&E.
- COTF continued the IOT&E with one RAM Block 2 missile firing scenario at the Naval Air Warfare Center, Point Mugu, California, in April 2016 from the Self-Defense Test Ship in accordance with a DOTE-approved test plan.

Assessment

- The classified March 2016 DOT&E Early Fielding Report, based on results of all completed IOT&E tests, stated that:
  - Insufficient data exist to characterize RAM Block 2's performance against all the ASCM threats the missile is intended to defeat. This condition will continue until the Navy completes the RAM Block 2 Probability of Raid

Annihilation modeling and simulation IOT&E phase, which is expected in late 2017.
- Completed testing has demonstrated that RAM Block 2 has demonstrated several improvements over its RAM Block 1 and 1A predecessors.
- Deficiencies in RAM Block 2 integration with the SSDS-based combat system caused several RAM Block 2 missiles to miss their target during one of the IOT&E missile firing scenarios.
- Due to the Navy's inability to develop an MSST, no assessment of RAM Block 2's capability against MSST-like ASCM threats is possible.
- The current steerable antenna system used on Navy aerial targets does not allow for an adequate emulation of specific ASCM threats.
- The Navy has not tested RAM Block 2's ability to home-on and destroy helicopter, slow aircraft, and surface threats thus no assessment of RAM Block 2's capability in this secondary mission area is possible.
- RAM Block 2 met its in-flight reliability requirement.

Recommendations

- Status of Previous Recommendations. The Navy has not completed the following previous recommendations:
  1. Correct the identified integration deficiencies with the SSDS-based combat system and RAM Block 2. Demonstrate these corrections in a phase of operational testing.
  2. Correct the SSDS scheduling function to preclude interference from prior intercepts and warhead detonations with RAM's infrared guidance. Demonstrate corrections in a phase of operational testing.
- FY16 Recommendations. The Navy should:
  1. Develop an MSST adequate for use in FOT&E. See the Test Resources section in this Annual Report for further details.
  2. Conduct FOT&E to determine RAM Block 2's capability to home-on and destroy helicopter, slow aircraft, and surface threats.
  3. Develop an improved steerable antenna system for its ASCM surrogates.

Ship Self-Defense for LHA(6)

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted a missile firing exercise on the Self-Defense Test Ship (SDTS) in April 2016. The SDTS was configured with the USS *America* (LHA 6) Ship Self-Defense System (SSDS)-based combat system. COTF conducted the test in accordance with a DOT&E-approved test plan. Results of testing completed to date continue to indicate that LHA 6 has some ship self-defense capability against older anti-ship cruise missile (ASCM) threats. LHA 6 ship self-defense performance against newer ASCM threats remains undetermined pending completion of the LHA 6 Probability of Raid Annihilation (PRA) modeling and simulation (M&S) test bed tests for IOT&E in late-2017.
- COTF conducted cybersecurity testing for the LHA 6 IOT&E and SSDS FOT&E on the LHA 6 in August 2016. Testing was conducted in accordance with a DOT&E-approved test plan. The test began with many known problems discovered during developmental testing in 2014 uncorrected. Data from the operational test are still being analyzed.

System

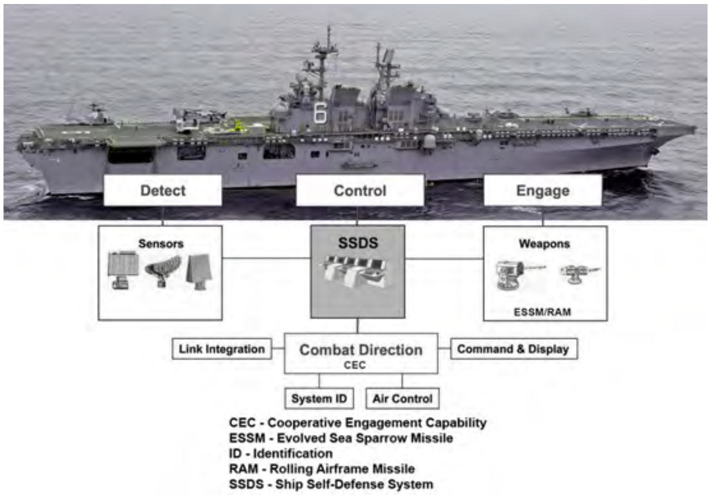
- Surface ship self-defense for the LHA 6 is addressed by several legacy combat system elements (including the AN-SPS-49A(V)1, AN/SPS-48E(V)10, and AN/SPQ-9B radars that are the primary self-defense radars) and five acquisition programs:
  - Ship Self-Defense System (SSDS)
  - Rolling Airframe Missile (RAM)
  - Evolved Seasparrow Missile (ESSM)
  - Cooperative Engagement Capability (CEC)
  - Surface Electronic Warfare Improvement Program (SEWIP)

SSDS

- SSDS is a local area network that uses open computer architecture and standard Navy displays to integrate a surface ship's sensors and weapons systems to provide an automated detect-track-engage sequence for ship self-defense.
- SSDS MK 1 is the legacy command and control system for LSD 41/49 class ships.
- SSDS MK 2 has six variants:
  - Mod 1, used in CVN 68 class aircraft carriers
  - Mod 2, used in LPD 17 class amphibious ships
  - Mod 3, used in LHD 7/8 class amphibious ships
  - Mod 4, used in LHA 6 class amphibious ships
  - Mod 5, used in LSD 41/49 class amphibious ships
  - Mod 6, in development for CVN 78 class aircraft carriers

RAM

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat ASCMs.



- There are three RAM variants:
  - RAM Block 0 uses dual-mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defense against ASCMs that do not emit radar signals.
  - RAM Block 2 adds kinematic and guidance improvements to extend the capability of RAM Block 1A against newer classes of ASCM threats.

ESSM

- The ESSM, cooperatively developed among 13 nations, is a medium-range, ship-launched, self-defense guided missile intended to defeat ASCM, surface, and low-velocity air threats.
- The ESSM is currently installed on LHA 6 and LHD 8 amphibious ships, DDG 51 Flight IIA destroyers, and CVN 68 class aircraft carriers equipped with the SSDS MK 2 Mod 1 Combat System.
- There are two variants of ESSM:
  - ESSM Block 1 is a semi-active radar-guided missile that is currently in service.
  - ESSM Block 2 is in development and will have semi active radar guidance and active radar guidance.

CEC

- CEC is a sensor network with an integrated fire control capability that is intended to significantly improve battle force air and missile defense capabilities by combining data from multiple battle force air search sensors on CEC-equipped units into a single, real-time, composite track picture.
- The two major hardware pieces are the Cooperative Engagement Processor, which collects and fuses radar data, and the Data Distribution System, which distributes CEC data to other CEC-equipped ships and aircraft.

- CEC is an integrated component of, and serves as the primary air tracker for, non-LSD class SSDS MK 2 equipped ships.
- There are two major surface ship variants of CEC:
  - The CEC AN/USG-2/2A is used in selected Aegis cruisers and destroyers, LPD 17/LHD/LHA 6 amphibious ships, and CVN 68 class aircraft carriers.
  - The CEC AN/USG-2B, an improved version of the AN/USG-2/2A, is used in selected Aegis cruisers/ destroyers as well as selected amphibious assault ships, including the LHA 6 ship class and CVN 68 class aircraft carriers.

SEWIP

- The SEWIP is an evolutionary development program providing block upgrades to the AN/SLQ-32 electronic warfare system to address critical capability, integration, logistics, and performance deficiencies.
- There are three major SEWIP block upgrades:
  - SEWIP Block 1, which is used on LHA 6 class ships, replaced obsolete parts in the AN/SLQ-32 and incorporated a new, user-friendly operator console, an improved electronic emitter identification capability, and an embedded trainer.
  - SEWIP Block 2 is in development and will incorporate a new receiver antenna system intended to improve the AN/SLQ-32's passive electronic warfare capability.
  - SEWIP Block 3 is in development and will incorporate a new transmitter antenna system intended to improve the AN/SLQ-32's active electronic warfare capability.

Mission

- Naval Component Commanders use SSDS, RAM, ESSM, SEWIP, and CEC, as well as many legacy systems, to accomplish ship self-defense missions.
- Naval surface forces use the:
  - SSDS to provide automated and integrated detect to engage ship self-defense capabilities against ASCM, air, and surface threats.
  - RAM to provide a short-range, hard-kill engagement capability against ASCM threats.
  - ESSM to provide a medium-range, hard-kill engagement capability against ASCM, surface, and low velocity air threats.
  - CEC to provide accurate air and surface threat tracking data to SSDS.
  - SEWIP-improved AN/SLQ 32 as the primary electronic warfare sensor and soft-kill weapons system for air defense (to include self defense) missions.

Major Contractors

- SSDS (all variants): Raytheon – San Diego, California
- RAM and ESSM (all variants): Raytheon – Tucson, Arizona
- CEC (all variants): Raytheon – St. Petersburg, Florida
- SEWIP
  - Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia
  - Block 2: Lockheed Martin – Syracuse, New York
  - Block 3: Northrop Grumman – Baltimore, Maryland

Activity

- COTF conducted a missile firing exercise on the SDTS in April 2016. The SDTS was configured with the USS *America* (LHA 6) SSDS-based combat system. This test, originally scheduled for early FY15, was postponed due to concerns over possible poor system performance.
- COTF conducted the test in accordance with a DOT&E-approved test plan
- COTF commenced cybersecurity testing for the LHA 6 IOT&E and the SSDS FOT&E on LHA 6 in August 2016 in accordance with a DOT&E-approved test plan; it is expected to complete in March 2017.
- COTF continued planning for the LHA 6 IOT&E PRA M&S test bed phase scheduled to commence in early-2017.

Assessment

- The April 2016 missile firing exercise on the SDTS resulted in the ESSM missile failing to destroy any of the threat surrogate targets. This failure was compounded by a combat system time synchronization problem that prevented the launch of a full salvo of ESSMs.
- Results of the April 2016 missile firing exercise on the SDTS identified deficiencies in SSDS processing of threat surrogate emitters and sensor detections; both of which could affect mission success.
- Results of testing completed to date continue to indicate that the LHA 6 has some ship self-defense capability against older ASCM threats. The LHA 6 ship self-defense performance against newer ASCM threats remains undetermined pending completion of the LHA 6 PRA M&S test bed runs for IOT&E in late-2017.
- Due to the Navy's inability to develop a Multi-Stage Supersonic Target (MSST), no assessment of the LHA 6 ship self-defense capability against MSST-like ASCM threats is possible.
- Final plans for operational testing and introduction of the Fire Control Loop Improvement Program (FCLIP) improvements in the LHA 6 ship class is unknown.
- Cybersecurity operational testing began with many known problems discovered during developmental testing in 2014

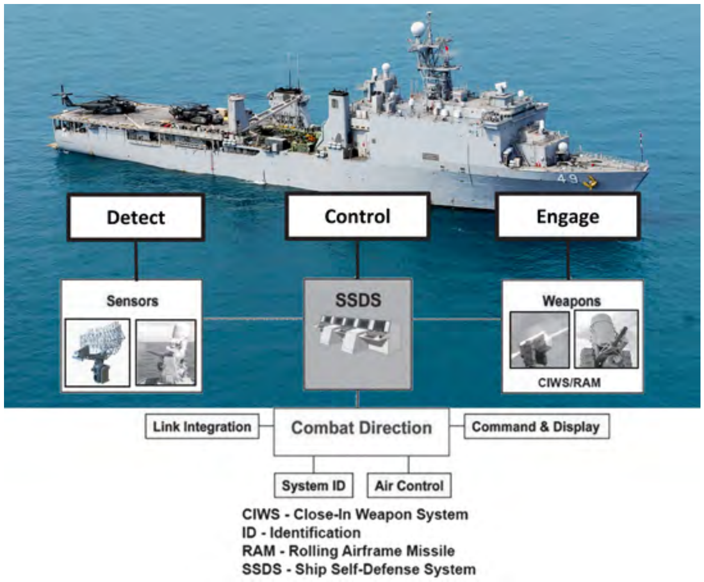
that were uncorrected. Data from the completed cybersecurity operational tests are still being analyzed.

- The Navy's reluctance to proceed with operational testing when it believes the outcome will unfavorably highlight poor performance is troubling because the ability of these ships' to defend themselves in a conflict is unknown and the root causes of any performance problems and the potential for correcting those problems also remains unknown.

Recommendations

- Status of Previous Recommendations. The Navy has satisfactorily completed some of the previous recommendations. However, the Navy has not resolved the following previous recommendations related to LHA 6 ship self-defense:
  1. Optimize SSDS MK 2 weapon employment timelines to maximize weapon Probability of Kill.
  2. Develop an adequate open-loop seeker subsonic ASCM surrogate target for ship self-defense combat system operational tests.
  3. Correct the identified SSDS MK 2 software reliability deficiencies.
  4. Correct the identified SSDS MK 2 training deficiencies.
  5. Develop and field deferred SSDS MK 2 interfaces to the Global Command and Control System – Maritime and the TPX-42A(V) command and control systems.
  6. Improve the ability of legacy ship self-defense combat system sensor elements to detect threat surrogates used in specific ASCM raid types.
  7. Improve the SSDS MK 2 integration with the MK 9 Track Illuminators to better support ESSM engagements.
  8. Develop combat system improvements to increase the likelihood that ESSM and RAM will home on their intended targets.
  9. Correct the cause of the ESSM missile failures and demonstrate the correction in a future phase of operational testing.
  10. Investigate means to mitigate the chances of an ESSM pre-detonating on debris before approaching its intended target.
  11. Investigate why target emitters continue to be reported as valid by the AN/SLQ-32 EWS with the SEWIP Block 1 upgrade after the target is destroyed. Test any corrections in a future operational test phase.
  12. Correct the SSDS scheduling function to preclude interference from prior intercepts and warhead detonations with RAM's infrared guidance. Demonstrate corrections in a phase of operational testing.
  13. Correct the integration problems with the SSDS-based combat system and the AN/SPQ-9B radar to ensure that all valid AN/SPQ-9B detections are used by the combat system when tracking targets. Demonstrate the corrections in a phase of operational testing.
- FY16 Recommendations. The Navy should:
  1. Complete the LHA 6 IOT&E at-sea test phase, cybersecurity testing, and the planning for the LHA 6 PRA M&S test bed IOT&E test phase.
  2. Update the LHA 6 and SSDS Test and Evaluation Master Plans to include at-sea and PRA test bed operational test phases to enable evaluation of the ship self-defense capabilities of the LHA 8 equipped with the new Enterprise Air Surveillance Radar.
  3. Continue to take action on the classified recommendations contained in the March 2011 and November 2012 DOT&E reports to Congress on the ship self-defense mission area.
  4. Provide a plan of action and milestones for introduction and operational testing of FCLIP improvements.
  5. Investigate and correct the cause of the ESSM missile failure to destroy any of the threat surrogate targets.
  6. Investigate and correct the combat system time synchronization problem that prevented the launch of a full salvo of ESSMs.
  7. Investigate and correct the SSDS processing of threat surrogate emitters and sensor detection deficiency.
  8. Develop an adequate MSST target as well as adequate electronic warfare target surrogates for use during operational testing. See the Test Resources section in this Annual Report for further details.

Ship Self-Defense for LSD 41/49



Executive Summary

- The Navy postponed gun and missile firing operational tests planned for June 2016 from the Self-Defense Test Ship (SDTS) equipped with the Ship Self-Defense System (SSDS) MK 2 Mod 5 Combat System due to initial concerns about possible poor performance and the desire to conduct detailed predictive analysis before proceeding with testing.
- The Navy's detailed predictive analysis is scheduled for completion in October 2016. A total of four missile firing and two gun firing operational test scenarios from the SDTS are planned. One missile firing scenario from the SDTS is scheduled for December 2016. The remaining three missile firing and two gun firing operational test scenarios from the SDTS are scheduled for no earlier than FY19.
- DOT&E intends to issue an SSDS MK 2 Mod 5 Early Fielding Report to Congress once the first SSDS MK 2 Mod 5-equipped LSD 41/49 ship deploys in late 2016. An additional two SSDS MK 2 Mod 5-equipped LSD 41/49 ships are planned to deploy in FY17 with at least one more planned to deploy in FY18. The report will state that there is a paucity of operational test results to support any assessment of the self- defense capabilities of the LSD 41/49 class ships equipped with the SSDS MK 2 Mod 5 Combat System and that the Navy is deploying those ships with unknown self-defense capabilities.

System

- Surface ship self-defense for the LSD 41/49 class ship is addressed by several legacy combat system elements (including the AN/SPS-49A(V)1 and Close-in Weapon System Radars that are the primary self-defense radars) and three acquisition programs:
  - Ship Self-Defense System (SSDS)
  - Rolling Airframe Missile (RAM)
  - Surface Electronic Warfare Improvement Program (SEWIP)

SSDS

- SSDS is a local area network that uses open computer architecture and standard Navy displays to integrate a surface ship's sensors and weapons systems to provide an automated detect-track-engage sequence for ship self defense.
- SSDS MK 1 is the legacy command and control system for LSD 41/49 class ships.
- SSDS MK 2 has six variants:
  - Mod 1, used in CVN 68 class aircraft carriers
  - Mod 2, used in LPD 17 class amphibious ships
  - Mod 3, used in LHD 7/8 class amphibious ships
  - Mod 4, used in LHA(R) class amphibious ships
  - Mod 5, used in LSD 41/49 class amphibious ships
  - Mod 6, in development for CVN 78 class aircraft carriers

RAM

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat anti-ship cruise missiles (ASCMs).
- There are three RAM variants:
  - RAM Block 0 uses dual-mode, passive radio frequency/ infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defense against ASCMs that do not emit radar signals.
  - RAM Block 2 adds kinematic and guidance improvements to extend the capability of RAM Block 1A against newer classes of ASCM threats.

SEWIP

- The SEWIP is an evolutionary development program providing block upgrades to the AN/SLQ-32 electronic warfare system to address critical capability, integration, logistics, and performance deficiencies.
- There are three major SEWIP block upgrades:
  - SEWIP Block 1, which is used on LSD 41/49 class ships, replaced obsolete parts in the AN/SLQ-32 and incorporated a new, user-friendly operator console, an improved electronic emitter identification capability, and an embedded trainer.
  - SEWIP Block 2 incorporates a new receiver antenna system intended to improve the AN/ SLQ-32's passive electronic warfare capability.

- SEWIP Block 3 is in development and will incorporate a new transmitter antenna system intended to improve the AN/SLQ-32's active electronic warfare capability.
- SEWIP-improved AN/SLQ 32 as the primary electronic warfare sensor and soft-kill weapons system for air defense (to include self defense) missions.

Mission

- Naval Component Commanders use SSDS, RAM, and SEWIP, as well as many legacy systems, to accomplish ship self-defense missions.
- Naval surface forces use the:
  - SSDS to provide automated and integrated detect to engage ship self-defense capabilities against ASCM, air, and surface threats.
  - RAM to provide a short-range hard-kill engagement capability against ASCM threats.

Major Contractors

- SSDS (all variants): Raytheon – San Diego, California
- RAM (all variants): Raytheon Missile Systems – Tucson, Arizona; RAMSys – Ottobrunn, Germany
- SEWIP
  - Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia
  - Block 2: Lockheed Martin – Syracuse, New York
  - Block 3: Northrop Grumman – Baltimore, Maryland

Activity

- The Navy postponed gun firing and missile firing operational tests planned for June 2016 from the SDTS equipped with the SSDS MK 2 Mod 5 Combat System due to initial concerns about possible poor performance and the desire to conduct detailed predictive analysis before proceeding with testing.
- The Navy's detailed predictive analysis is scheduled for completion in October 2016. A total of four missile firing and two gun firing operational test scenarios from the SDTS are planned. One missile firing scenario from the SDTS is scheduled for December 2016. The remaining three missile firing and two gun firing operational test scenarios from the SDTS are scheduled for no earlier than FY19.
- The first SSDS MK 2 Mod 5-equipped LSD 41/49 ship deploys in late 2016. An additional two SSDS MK 2 Mod 5-equipped LSD 41/49 ships are planned to deploy in FY17 with at least one more planned to deploy in FY18.

Assessment

- The Navy's reluctance to proceed with any operational testing as scheduled in June 2016 over concerns of highlighting poor system performance is troubling because the ability of these deploying ships' to defend themselves in a conflict is unknown and the root causes of any performance problems and the potential for correcting those problems also remains unknown. The resulting delay now allows for conduct of only one of the six required missile/gun firing operational tests (December 2016) to support deployments of the first four LSD 41/49 ships equipped with the SSDS MK 2 Mod 5 Combat System. There is, therefore, a paucity of operational test results to support any assessment of the self-defense capabilities of the LSD 41/49 class ships equipped with the SSDS MK 2 Mod 5 Combat System and the Navy is deploying these ships with unknown self-defense capabilities. The assessment of the self-defense capabilities of the LSD 41/49 class ship equipped with the SSDS MK 2 Mod 5 Combat System cannot be completed until all planned operational tests are conducted. SDTS scheduling constraints will delay completion of the remaining five required missile/gun firing operational tests until FY19 at the earliest when most, if not all, LSD 41/49 ships equipped with the SSDS MK 2 Mod 5 Combat System will have been deployed.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendation.
  1. The Navy should complete all planned operational tests of the LSD 41/49 ship class equipped with the SSDS MK 2 Mod 5 Combat System as soon as possible and prior to further ship deployments.

Ship-to-Shore Connector (SSC)

Executive Summary

- Ship-to-Shore Connector (SSC) delays have resulted in a delivery of the first craft, designated as the test and training craft, at the end of FY17. IOT&E is scheduled for mid-FY19, with Initial Operational Capability planned for FY20. LFT&E events to assess susceptibility of the craft to naval mines, controlled damage test to determine the ability to maintain mission capability following damage from a threat weapon, and seaworthiness testing to verify the modeling results from scale model testing conducted in FY13 are also delayed until FY18. The data and analysis necessary to inform a Full-Rate Production decision will not be available until the end of FY19. The Navy intends to go into full-rate production in FY19.
- In FY16, the Navy completed the data analysis of the live fire full-hull tests conducted in 2015 on the legacy Landing Craft Air Cushion (LCAC), the approved surrogate for this test. This full-scale test data informs the continuing refinement of the models needed to assess the vulnerability of the SSC and personnel to surf-zone mines, fragmenting artillery rounds, and land mines.
- An initial analysis of the live fire full-hull test data confirmed the need for follow-on component tests to aid in determining the survivability of the platform and crew. Additional live fire events are planned for FY17.

System

- The SSC is a fully amphibious air cushion vehicle intended to replace the existing LCACs.
- Compared to the existing LCAC, the Navy intends the SSC to have increased payload, reliability, and availability.
- The Navy intends to operate the SSC from the well decks of current and planned Navy amphibious ships and onboard the planned Mobile Landing Platform.

- The SSC has ballistic/fragmentation protection for manned crew and embarked troop spaces, various installed and portable damage control and firefighting systems intended to support recoverability from peacetime fire and flooding casualties
- The SSC is designed to carry a crew of 5 and up to 26 passengers with their combat equipment.

Mission

Commanders will employ amphibious forces equipped with the SSC to transport equipment, personnel, and weapons systems from ships through the surf zone and across the beach to landing points in support of amphibious operations worldwide.

Major Contractor

Textron Systems – New Orleans, Louisiana

Activity

- In FY16, the Navy completed the analysis of the full-hull test data collected using an operational LCAC (as a surrogate for the SSC) against a surf-zone mine emplaced under the skirt, an under-hull land mine, and a blast and fragmentation threat. The Navy is using the data to refine the kill criteria used for the SSC vulnerability modeling and simulations. The Navy is preparing a Vulnerability Assessment Report (VAR) with the revised kill criteria from the surrogate testing. This VAR was due in FY16, but the Navy has adjusted the delivery date to the end of CY16. Delays in completing this report and production delays may jeopardize the planning for the controlled damage test planned in FY17 and FY18.
- The 2015 full-hull test data review confirmed the need to conduct additional testing on the propulsion power plant components. The Navy is in the process of planning this test for execution in FY17.
- The 2015 full-hull test data review confirmed the need to evaluate the potential for personnel injury in some of the installed SSC seats for a loading condition similar to those experienced during the test. While the SSC energy-attenuating seats were not available for installation in the Command Module for the full-hull test, the Navy collected data using the LCAC seats to facilitate future analysis on the performance of

new seats when these become available. The Navy is in the process of planning this test for execution in FY17.
- Armor characterization testing, originally scheduled for early FY16, was delayed in order to allow for the procurement of armor that meets the SSC specifications. The testing began in late FY16 with a partial delivery of armor test coupons and is expected to be completed in FY17.

Assessment
- The SSC's ballistic/fragmentation protection for manned crew and embarked troop spaces, installed and portable damage control and firefighting systems provide limited capability for recoverability from battle damage incurred during combat.
- The preliminary analysis of the full-hull testing data collected in FY15 identified data that can be used to refine craft damage predictions and crew and troop casualty predictions. DOT&E will assess the validity of this approach to support the final determination of the survivability of the SSC and the crew in FY19.
- The SSC propulsion plant is different from the legacy LCAC, which was used in the full-hull tests. It shares the MV-22 power plant; however, the SSC shafts are larger and have different composite material composition. Based on the full-hull test data review, DOT&E concurs with the Navy's proposal to execute a test to further assess the response of the propulsion plant composite shafts to weapon effects because such data are not available from historical tests (conducted for helicopters and the MV-22). DOT&E will review the proposed test plan for adequacy in FY17.
- While the SSC has energy-absorbing seats for the pilot and co-pilot, these are designed to mitigate the loading condition to the body during normal operation of the craft. The full-hull test confirmed the need to assess the significance of loading conditions to the occupants of these seats following an under hull blast event. DOT&E will review the proposed test plan for adequacy in FY17.
- The Navy is conducting armor characterization testing in accordance with the DOT&E-approved test plan.

Recommendations
- Status of Previous Recommendations. The Navy has addressed some of the FY15 recommendations. It evaluated the results of the full-hull tests and determined that additional component tests were warranted. The Navy is currently planning two additional test series to include the propulsion plant composite shaft tests and energy-absorbing seat tests. However, it still needs to address the outstanding FY15 recommendation to evaluate the classified findings from the full-hull test to determine if the risk for personnel casualties can be reduced.
- FY16 Recommendation.
  1. The Navy should complete and deliver the VAR to DOT&E in FY17 to enable adequate planning of remaining live fire test series and determination of platform survivability.

SSN 774 *Virginia* Class Submarine

Executive Summary

- The Navy deployed the first *Virginia* class Block III submarine, USS *North Dakota* (SSN 784), in May 2015, with only limited developmental testing of the platform's major subsystem upgrades. Major testing phases included developmental testing of the new Large Aperture Bow (LAB) sonar array, testing of the system to support weapon system accuracy (this included sonar performance assessments), testing of the weapon system interfaces, and a limited operational assessment phase to support deployment certification.
- DOT&E submitted a classified Early Fielding Report in September 2015 detailing the results of the testing to date. DOT&E concluded that:
  - The *Virginia* class Block III submarine with the LAB array has the potential to perform as an adequate replacement for the spherical array used on previous *Virginia* class variants.
  - System reliability meets the Navy's thresholds.
  - The new LAB array and the Light Weight Wide Aperture Array (LWWAA) sonar processing systems suffer from some deficiencies. Although the Navy has implemented corrective action in each case, a full operational evaluation has not yet been conducted.
- The Navy commenced a cybersecurity assessment of the *Virginia* class Block III submarine in September 2016. The Navy intends to complete a comprehensive operational test of the *Virginia* class Block III submarine in FY17 that covers anti-submarine warfare, anti-surface ship warfare, strike warfare, and intelligence collection mission areas.

System

- The *Virginia* class submarine is the Navy's latest fast attack submarine and is capable of targeting, controlling, and launching MK 48 Advanced Capability torpedoes and Tomahawk cruise missiles.
- The Navy is procuring *Virginia*-class submarines incrementally in a series of blocks; the block strategy is for contracting purposes, not necessarily to support upgrading capabilities.
  - Block I (hulls 1-4) and Block II (hulls 5-10) ships were built to the initial design of the *Virginia* class.
  - Block III (hulls 11-18) and Block IV (hulls 19-28) ships include the following affordability enhancements starting with SSN 784, USS *North Dakota*:
    - A LAB array in place of the spherical array in the front of the ship.
    - Two *Virginia* payload tubes replace the 12 vertical launch tubes; each payload tube is capable of storing and launching six Tomahawk land attack missiles used in strike warfare missions.
  - Block V and beyond will increase strike payload capacity from 12 to 40 Tomahawk land attack missiles by adding a set of four additional payload tubes in an amidships payload module, capable of storing and launching seven Tomahawk missiles each, as well as providing the potential to host future weapons and unmanned systems.

Mission

The Operational Commander will employ the *Virginia* class Block III submarine to conduct open-ocean and littoral covert operations that support the following submarine mission areas:

- Strike warfare
- Anti-submarine warfare
- Intelligence, surveillance, and reconnaissance
- Mine warfare
- Anti-surface ship warfare
- Naval special warfare
- Battle group operations

Major Contractors

- General Dynamics Electric Boat – Groton, Connecticut
- Huntington Ingalls Industries, Newport News Shipbuilding – Newport News, Virginia

Activity

- The Navy completed the shock qualification testing for the *Virginia* Common Weapons Launcher and the *Virginia* Payload Tube hatch in late 2014, but has since redesigned a subcomponent of the hatch. Electric Boat has requested hatch shock qualification with a noted exception of the modified component and is investigating methods to resolve this exception. The Navy is evaluating, but has not yet approved, the request.
- In September 2015, DOT&E submitted a classified Early Fielding Report on the first *Virginia* class Block III submarine due to submarine deployment prior to the completion of operational testing.
- The Navy continued its analysis, but delayed validation of the Transient Shock Analysis modeling method used for the design of *Virginia* class Block III items until FY17.
- The Navy delayed the update of the *Virginia* class Vulnerability Assessment report that addresses Block III modifications until FY17.
- In September 2016, the Navy commenced a cybersecurity assessment of the *Virginia* class Block III submarine in accordance with a DOT&E-approved test plan. The assessment will complete in FY17.
- The Navy intends to complete a comprehensive operational test of the *Virginia* class Block III submarine in FY17 that covers anti-submarine warfare, anti-surface ship warfare, strike warfare, and covert intelligence collection mission areas.

Assessment

- The September 2015 DOT&E classified Early Fielding Report details the impact of the new major components of the system with respect to the intended mission during the early deployment. The report concluded the following:
  - The changes to the *Virginia* class Block III submarine do not appear to improve or degrade the system's ability to conduct submarine missions.
  - The LAB array demonstrates the potential to perform as an adequate replacement for the legacy spherical array.
  - Although the technical parameters are similar, the system presented a series of display artifacts, which could affect performance. The Navy issued software fixes to mitigate the effects; however, the software remains to be operationally tested.
  - The sonar LWWAA experienced a hardware fault which limited the ability to assess effectiveness of the system.
  - Developmental testing of the system indicates that system software reliability meets the Navy's thresholds. Hardware reliability was not able to be evaluated because of the limited time available to testers for the evaluation. The LAB array outboard signal processing equipment has exhibited some early failures. The Navy issued fleet guidance for monitoring system performance and continues to investigate potential causes.
- The cybersecurity assessment of the *Virginia* class Block III submarine remains ongoing and will be reported in FY17.

Recommendations

- Status of Previous Recommendations. The following are recommendations that remain from FY15. The Navy should:
  1. Test against a diesel submarine threat surrogate in order to evaluate *Virginia's* capability, detectability, and survivability against modern diesel-electric submarines.
  2. Conduct an FOT&E to examine *Virginia's* susceptibility to airborne anti-submarine warfare threats such as Maritime Patrol Aircraft and helicopters.
  3. Coordinate the *Virginia*, Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI), and AN/BYG-1 Test and Evaluation Master Plans to facilitate testing efficiencies.
  4. Complete the verification, validation, and accreditation of the Transient Shock Analysis method used for *Virginia* class Block III items.
  5. Repeat the FOT&E event to determine *Virginia's* susceptibility to low-frequency active sonar and the submarine's ability to conduct anti-surface ship warfare in a low-frequency active environment. This testing should include a *Los Angeles* class submarine operating in the same environment to enable comparison with the *Virginia* class submarine.
  6. Investigate and implement methods to aid the Special Operation Forces in identifying the submarine during operations in conditions of low visibility.
  7. Address the three classified recommendations listed in the September 2015 Block III *Virginia* class Early Fielding Report.
- FY16 Recommendations. None.

Standard Missile-6 (SM-6)

Executive Summary

- The performance deficiency discovered during IOT&E and outlined in the May 2013 classified Standard Missile-6 (SM-6) IOT&E report remains unresolved and continues to affect DOT&E's final assessment of effectiveness.
  - The Navy is assessing several options for a solution, each with varying degrees of complexity. A primary concern is to ensure the solution causes no degradation to the existing SM-6 performance envelope.
  - The Navy plans to incorporate these changes in Block I (BLK I) and Block IA (BLK IA) production variants and conduct operational testing in FY17.
- In FY16, the Navy completed FOT&E live fire testing. These tests provided validation data for the modeling and simulation runs for the record phase of the FOT&E. The Navy intends to conduct the modeling and simulation tests in FY17, which will complete the SM-6 BLK I FOT&E.
- In FY16, the Navy successfully demonstrated the maximum range Key Performance Parameter (KPP) and the launch availability Key System Attribute during SM-6 BLK I FOT&E and Aegis Baseline 9 operational testing.
- The Navy commenced developmental testing of pre-planned product improvements to the SM-6 BLK I missile in FY14; these improvements are the SM-6 BLK IA configuration. The Navy conducted a successful developmental test of the SM-6 BLK IA Guidance Test Vehicle (GTV) mission (GTV-3) in FY16. The Navy plans to conduct operational testing of the SM-6 BLK IA in FY17.
- The Navy conducted six SM-6 BLK I missile tests during FY16. Of the planned launches, four successfully supported FOT&E with Aegis Baseline 9; one test successfully supported Navy Integrated Fire Control – Collateral (NIFC-CC) Demonstration; one Agile Prism developmental test launch was unsuccessful.
- The uplink/downlink antenna shroud reliability problem discovered in IOT&E has been resolved; 34 production missiles with the new design have been fired without failure.
- NIFC – Counter Air (CA) From-the-Sea (FTS) Increment I became a fielded capability in 2015 and fully integrated as a tactical option in fleet air defense. Future testing of the Advanced Capability Build (ACB) 16 and ACB 20 Aegis Modernizations and SM-6 will evaluate the NIFC-CA FTS Increment II capability.

System

- SM-6 is the latest evolution of the Standard Missile family of fleet air defense missiles.
- The Navy employs the SM-6 from cruisers and destroyers equipped with the Aegis combat systems.
- The SM-6 seeker and terminal guidance electronics derive from technology developed in the Advanced Medium-Range Air-to-Air Missile program.
- SM-6 retains the legacy Standard Missile semi-active radar homing capability.
- SM-6 receives midcourse flight control from the Aegis Combat System (ACS) via ship's radar; terminal flight control is autonomous via the missile's active seeker or supported by the ACS via the ship's illuminator.
- The Navy is upgrading SM-6 to the BLK I configuration to address hardware and software improvements and to address advanced threats.
- SM-6 Dual I capability is being added to provide Sea-Based Terminal capability against short-range ballistic missiles.
- The Navy is upgrading the SM-6 to add an anti-surface target capability.

Mission

- The Joint Force Commander/Strike Group Commander will employ naval units equipped with the SM-6 for air defense against fixed-/rotary-winged targets and anti-ship missiles operating at altitudes ranging from very high to sea skimming.
- The Joint Force Commander will use SM-6 as part of the NIFC-CA FTS operational concept to provide extended range over-the-horizon capability against at-sea and overland threats.
- The Joint Force Commander will use SM-6 as part of the NIFC-CC operational concept to provide extended range capability against surface targets.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- The Navy conducted six SM-6 BLK I missile tests during FY16. Of the planned launches, four successfully supported FOT&E with Aegis Baseline 9, one successfully supported the NIFC-CA Tactical Demonstration, but one supporting the Aegis Agile Prism demonstration was unsuccessful.

SM-6 BLK I FOT&E

- In January 2016, at the Pacific Missile Range Facility, Kauai, Hawaii:
  - An SM-6 BLK I FOT&E mission (D1A) successfully engaged a maximum downrange target.
  - An SM-6 BLK I FOT&E mission (D1B) successfully engaged a maximum cross-range target.
  - An SM-6 BLK I FOT&E mission (D1D) successfully engaged two SM-6s against two subsonic targets. An Aegis Weapon Control System integration problem appeared that did not affect the mission.
  - An SM-6 BLK I FOT&E mission (D1Ga) successfully engaged a target that was using electronic attack against the SM-6.
- The Navy conducted the FOT&E in accordance with the DOT&E-approved test plan.

Navy Integrated Fire Control – Collateral (NIFC-CC) Demonstration

- In January 2016, at the Pacific Missile Range Facility, the Navy successfully conducted the SM-6 NIFC-CC Demonstration mission.

Navy Integrated Fire Control – Counter Air From the Sea Increment I (NIFC-CA FTS Increment I)

- In September 2016, at White Sands Missile Range, New Mexico, the Navy and Marine Corps successfully conducted a NIFC-CA FTS Increment I demonstration event using an F-35 Lightning II as a targeting source for the Aegis BL9 Desert Ship test configuration and the SM-6. This demonstration was developmental testing and did not represent a fleet operational configuration of the ACS or all the required communications links. The demonstration used a non-tactical engineering computer software build in the Aegis Desert Ship test site, itself not fully representative of the ACS, interfaced to a datalink gateway that could receive the F-35 Multifunction Advanced Data Link (MADL) and port track data from the aircraft sensor to the AWS. Using this track data, an SM-6 was initialized and launched at an MQM-107 unmanned target drone.
- In September 2016, at the Pacific Missile Test Center, California, the Navy conducted an at-sea flight demonstration of the NIFC-CA FTS Increment I.

AGILE PRISM

- In March 2016, at the Pacific Missile Range Facility, an SM-6 BLK 1 missile did not successfully engage either of the two threat targets at low altitude during a developmental test event.

SM-6 BLK IA

- The Navy commenced developmental testing of pre-planned product improvements to the SM-6 BLK I missile in FY14; these improvements are the SM-6 BLK IA configuration. The Navy conducted a successful developmental test of the SM-6 BLK IA Guidance Test Vehicle (GTV) mission (GTV-3) in FY16. The Navy plans to conduct operational testing of the SM-6 BLK IA in FY17.

Assessment

- In FY16, the Navy completed FOT&E live fire testing. These tests provided validation data for the modeling and simulation runs for the record phase of the FOT&E. The Navy will conduct this phase of test during FY17, which will complete the SM-6 BLK I FOT&E.
- During FY16 flight tests, there were no occurrences of the uplink/downlink antenna shroud reliability deficiency. DOT&E considers the uplink/downlink antenna shroud reliability deficiency to be resolved. To date, the Navy has fired 34 SM-6s with full production antennas with no observations of anomalies. At the 80 percent confidence level, the reliability of the antennas is at least 95.4 percent.
- The March 2015 SM-6 BLK I mission D1G misfire remains under investigation by the Navy with no root cause determination to date.
- In the May 2013 SM-6 IOT&E report, DOT&E assessed SM-6 BLK I as suitable. This assessment considered combined data from the IOT&E and developmental/operational flight tests. During FY16 testing, DOT&E collected additional reliability data and assessed that the SM-6 BLK I continues to remain suitable. DOT&E will continue to collect suitability and effectiveness data throughout SM-6 BLK IA FOT&E testing in FY17, as well as during all SM-6 flight testing in support of NIFC-CA FTS, Missile Defense Agency, and Aegis software baseline development.
- The performance deficiency discovered during IOT&E and outlined in the classified IOT&E report remains unresolved and continues to affect DOT&E's final assessment of effectiveness. The Navy is assessing several options for a solution, each with varying degrees of complexity. A primary concern is to ensure the solution causes no degradation to the existing SM-6 performance envelope. The corrective actions will be incorporated into production of the SM-6 BLK I and BLK IA configurations and tested during FOT&E in FY17.
- In FY16, the Navy successfully demonstrated the maximum range KPP during SM-6 FOT&E and the maximum cross-range Key System Attribute.
- DOT&E assesses the launch availability KPP to be resolved. The Navy stored seven missiles aboard an operational ship for at least 8 months prior to firing during FOT&E with no launch availability problems noted. This yields a launch availability of 1.0 with an 80 percent confidence lower bound of 0.81, against a requirement of 0.98.
- Upon completion of the SM-6 FOT&E in FY17, the Navy will have conducted sufficient testing to allow an assessment of the SM-6 Capability Production Document performance requirement for interoperability.
- The failure during the Aegis Agile Prism test remains under investigation by the Navy.

- The Navy's NIFC-CA FTS Increment I test events conducted to date were sufficient to demonstrate basic capability; however, these demonstrations were not conducted under operationally realistic conditions or against aerial targets representative of modern threats. Additionally, the scenarios conducted were not sufficiently challenging to demonstrate the NIFC-CA FTS requirements defined in the Navy's September 2012 NIFC-CA FTS Testing Capability Definition Letter. Nevertheless, since NIFC-CA FTS Increment I has been fully integrated as a tactical option in fleet air defense, DOT&E removed the NIFC-CA FTS, as a distinct program, from test and evaluation oversight. DOT&E will assess and report NIFC-CA FTS (Increment II) performance as part of the FY18-23 ACB 16 and ACB 20 Aegis Modernization operational testing and SM-6 FOT&E.
- In September 2016, at White Sands Missile Range, the Navy and Marine Corps successfully conducted a NIFC-CA FTS Increment I demonstration event using an F-35 Lightning II as a targeting source to allow the ACS (partial) installed at the Desert Ship test facility to engage an aerial target with the SM-6. The configuration of the F-35 and the Desert Ship was not operationally representative and not all the required communications links were present. This demonstration was part of developmental testing and did not represent a fleet operational configuration of the ACS. The demonstration used a non-tactical engineering computer software build in the Aegis Desert Ship test site – itself not fully representative of the ACS – interfaced to a datalink gateway that could receive the F-35 MADL and port track data from the aircraft sensor to the AWS. Using these track data, an SM-6 successfully engaged an MQM-107 unmanned target drone. This demonstration was conducted as a proof of concept to show that the NIFC-CA FTS Increment I capability could utilize additional airborne sensors to provide fire control quality data to the AWS. In the context of the event, this objective was met; however, this demonstration should not be construed as an operational capability.
- In September 2016, at the Pacific Missile Test Center, the Navy successfully conducted an at-sea flight demonstration of the NIFC-CA FTS Increment I. This test resulted in the longest-range SM-6 interception to-date.

Recommendations

- Status of Previous Recommendations. The Navy is addressing the previous recommendations from FY14 to complete corrective actions of the classified performance deficiency discovered during IOT&E and develop a flight test program to test those corrective actions. The Navy plans to conduct verification flight tests in FY17. The Navy has not addressed the FY15 recommendation; however, this recommendation is rescinded as NIFC-CA FTS Increment I has been fully integrated as a tactical option in fleet air defense, DOT&E removed the NIFC-CA FTS, as a distinct program, from test and evaluation oversight and will be tested as a normal tactic in future Aegis/SM-6 testing.
- FY16 Recommendations. None.

Surface Electronic Warfare Improvement Program (SEWIP) Block 2

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted IOT&E in March and June 2016, on USS *Bainbridge* (DDG 96) in the Virginia Capes operating area in accordance with a DOT&E-approved test plan.
- DOT&E submitted a classified IOT&E report in September 2016 to Congress on the results of the IOT&E for the AN/SLQ-32 Electronic Warfare System (EWS) equipped with the Surface Electronic Warfare Improvement Program (SEWIP) Block 2 upgrade. The analysis showed that the SEWIP Block 2 upgrade was operationally effective but not operationally suitable or survivable.

System

- SEWIP is an incremental development program that is intended to improve the electronic warfare capability on all Navy surface combatants.
- The SEWIP Block 2 upgrade incorporates a new antenna system and enhanced processing capabilities into the AN/SLQ-32 EWS, which are intended to improve the AN/SLQ-32's passive electronic support capabilities.

Mission

Commanders employ Navy surface ships equipped with SEWIP Block 2 to enhance the AN/SLQ-32 EWS anti-ship missile defense, counter-targeting, and counter surveillance capabilities and to improve the system's ability to collect electronic data.

Major Contractor

SEWIP Block 2: Lockheed Martin – Syracuse, New York

Activity

- COTF conducted the IOT&E in March and June 2016, on USS *Bainbridge* (DDG 96) in the Virginia Capes operating area.
- DOT&E submitted a classified IOT&E report in September 2016 to Congress on the results of the IOT&E for the AN/SLQ-32 EWS equipped with the SEWIP Block 2 upgrade.

Assessment

- Analysis of the IOT&E data showed the SEWIP Block 2 to be operationally effective.
- Analysis of the IOT&E data showed the SEWIP Block 2 to be not operationally suitable due to:
  - Poor software reliability.
  - Insufficient data were collected during the IOT&E to fully assess the SEWIP Block 2 hardware reliability.
  - Fleet operators were not being adequately trained to operate and maintain the system.
  - Although the Mean Time to Reboot met the requirement of 18 minutes, it took 8 minutes on average, which is a significant amount of time if a reboot occurs during an anti-ship cruise missile attack.
- Analysis of the IOT&E data showed that the SEWIP Block 2 to be not survivable due to cybersecurity deficiencies.

Recommendations

- Status of Previous Recommendations. The Navy has not resolved the following SEWIP FY06 and FY08 previous recommendations to:
  1. Continue to review and modify the SEWIP software to improve its reliability.
  2. Develop threat representative aerial target/threat seeker combinations and/or procure actual threat anti-ship cruise missiles for more realistic operational testing of future SEWIP block upgrades and other EWSs.
- FY16 Recommendations. The Navy should:

1. Review and modify the SEWIP Block 2 software to improve its reliability and test the modifications in a phase of FOT&E.
2. Improve the SEWIP Block 2 training so fleet operators can effectively operate and maintain the system.
3. Improve the SEWIP Block 2 Mean Time to Reboot times and test those improvements in a phase of FOT&E.
4. Gather hardware reliability data from fleet units equipped with SEWIP Block 2 to enable a full assessment of hardware reliability.
5. Take action on the recommendations contained in the classified September 2016 DOT&E IOT&E report.
6. Correct the cybersecurity deficiencies and test those corrections in an FOT&E phase.

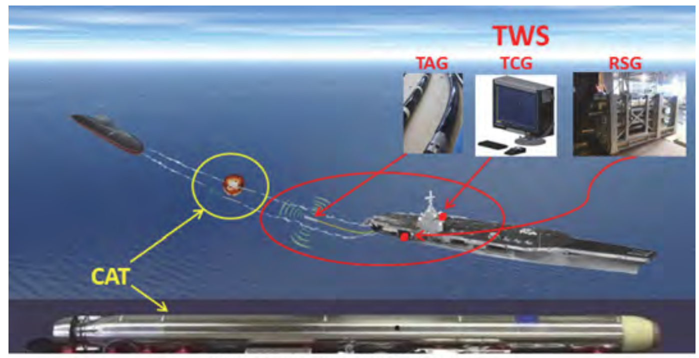
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT)

Executive Summary

- USS *Dwight D. Eisenhower* commenced deployment in 3QFY16 with a temporary roll-on/roll-off version of the Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT) referred to as the Anti-Torpedo Torpedo (ATT) Defense System (ATTDS). Like previous carrier deployments, the *Dwight D. Eisenhower* deployed with a passive only TWS array.
- USS *Theodore Roosevelt* returned from deployment in 1QFY16 and USS *Harry S. Truman* returned from deployment later in 3QFY16. During these deployments, the crews rarely deployed the TWS arrays; thus, little data were collected to determine the TWS arrays' reliability or to assist the developer with improving its detection, tracking, alerting, and false alert rejection software.
- A combined TWS and CAT contractor test in July 2016 demonstrated the Navy's contractors are making progress toward developing an initial defensive capability to counter a salvo of threat torpedoes and improving the active source reliability. The test demonstrated that the TWS active and passive system, with a highly qualified sensor operator, is capable of detecting, tracking, and alerting on threat torpedoes; that operators can initiate a salvo of CATs to intercept the threat torpedoes; and that a salvo of CATs can intercept a salvo of threat torpedoes.

System

- Surface Ship Torpedo Defense is a system of systems that includes two new sub-programs: the TWS (an Acquisition Category III program) and CAT (will not become an acquisition program until FY17). Combined, TWS and CAT are referred to as the ATTDS.
- TWS is being built as an early warning system to detect, localize, classify, and alert on incoming threat torpedoes and consists of three major subsystems:
  - The Target Acquisition Group consists of a towed acoustic array, tow cable, winch, power supply, and signal processing equipment. Data from the array and the ship's radar system are processed into contact tracks and alerts to be forwarded to the Tactical Control Group. The Navy intends the array to be capable of both passive and active sonar operations.
  - The Tactical Control Group consists of duplicate consoles on the bridge and Combat Direction Center (on CVNs) that displays contacts, issues torpedo alerts to the crew, and automatically develops CAT placement presets using information sent from the Target Acquisition Group.



CAT - Countermeasure Anti-Torpedo
RSG - Ready Stow Group
TAG - Target Acquisition Group
TCG - Tactical Control Group
TWS - Torpedo Warning System

  The operator uses these displays to manage the threat engagement sequence and command CAT launches.
  - The Ready Stow Group will consist of the steel cradles housing the CATs. The permanent system consists of four steel cradles and associated electronics, each housing six ATTs at different locations (port/starboard and fore and aft on the CVN).
- CAT is a hard-kill countermeasure intended to neutralize threat torpedoes and consists of the following:
  - The ATT is a 6.75-inch diameter interceptor designed for high-speed and maneuverability to support rapid engagement of the threat torpedo.
  - The All-Up Round Equipment consists of a nose sabot, ram plate, launch tube, muzzle cover, breech mechanism, and energetics to encapsulate and launch the ATT.
  - The tactical CAT is powered by a Stored Energy Propulsion System (SCEPS). The battery-powered electric motor CAT is for test purposes only. Engineering Development Model (EDM)-2 is the current hardware version of the CAT.
- The Navy developed a temporary version of TWS and CAT (designated a roll-on/roll-off system) in addition to the permanent-installation version. The Navy intends for this version to provide the same functionality as the permanent one.
  - The Ready Stow Group steel cradles are replaced by two lighter-weight and less-robust aluminum Launch Frame Assemblies that each hold four CATs.
  - The processing required for the Target Acquisition Group and the Tactical Control Group resides in two cabinets

contained in a container express box located on the carrier's hangar deck.
- The towed acoustic array, tow cable, and winch are permanently installed on the carrier's fantail. The other components of the system, including the operator displays and fire enable switch, reside in the container express box located on the hangar deck.

Mission

Commanders of nuclear-powered aircraft carriers and Combat Logistic Force ships will use the Surface Ship Torpedo Defense system to defend against incoming threat torpedoes.

Major Contractors

TWS

- Ultra Electronics-3Phoenix – (Prime Contractor) – Chantilly, Virginia, and Wake Forest, North Carolina
- Alion Science and Technology – (Acoustics and testing consultant) – New London, Connecticut
- In-Depth Engineering – (Tactical Control Group software development) – Fairfax, Virginia
- Pacific Engineering Inc. (PEI) – (Ready Stow Group manufacture) – Lincoln, Nebraska
- Rolls-Royce – (Winch manufacture) – Ontario, Canada
- Teledyne – (Towed Array manufacture and assembly) – Houston, Texas

CAT

- Pennsylvania State University Applied Research Laboratory – (ATT Systems) – State College, Pennsylvania
- Pacific Engineering Inc. (PEI) – (Canister fabrication) – Lincoln, Nebraska
- SeaCorp – (All Up Round Equipment fabrication and assembly) – Middletown, Rhode Island

---

Activity

- In August 2015, the Naval Surface Warfare Center, Indian Head Explosives Ordnance Disposal Technology Division, conducted ATT warhead and safety and arming device airburst testing at Fort A.P. Hill, Virginia. This testing verified the arming, fuzing, and firing of the ATT warhead.
- During FY16, the Navy and DOT&E continued development of an enterprise Test and Evaluation Master Plan (TEMP) for the TWS and CAT systems. The Navy made their TWS Milestone B decision without a TEMP; they are not planning to make the CAT system an acquisition program until later in FY17.
- USS *Theodore Roosevelt* returned from deployment in 1QFY16. The *Theodore Roosevelt* deployed with a temporary roll-on/roll-off version of the TWS and CAT. During the deployment, the crew rarely deployed the TWS array.
- In February/March 2016, the Navy and Pennsylvania State University Applied Research Laboratory conducted contractor testing of CAT on the Dabob Bay, Washington, acoustic tracking range. The testing consisted of three highly scripted scenarios to obtain data and evaluate the salvo capability of the CATs. During this test, both the threat torpedo target surrogates and the ATTs were fired from a single test platform (torpedo retriever). The target surrogates ran a scripted geometry and the ATTs ran tactical profiles to intercept the threat surrogates.
- USS *Dwight D. Eisenhower* commenced deployment in 3QFY16 with a temporary roll-on/roll-off version of TWS and CAT that includes the TWS Target Acquisition Group and the Tactical Control Group hardware and two of the four planned CAT Ready Stow Group cradles containing eight CAT EDM-2s powered by SCEPS. Like previous carrier deployments, the Towed Active Acoustic Source (TAAS) was not ready and the *Dwight D. Eisenhower* deployed with a passive-only TWS array. Ultra-Electronics-3Phoenix contractor personnel deployed aboard the *Dwight D. Eisenhower* to operate and maintain the TWS system, train Navy operators, and to collect system data. The Navy Program Office intends *Dwight D. Eisenhower* to be the last carrier to receive the temporary installation and is planning the installation of the permanent version of the TWS and CAT early fielded hardware on selected CVNs before their next deployments.
- USS *Harry S. Truman* returned from deployment later in 3QFY16. The *Harry S. Truman* has a permanent installation of TWS and CAT that includes the TWS Target Acquisition Group and the Tactical Control Group hardware and two of the four planned CAT Ready Stow Group steel cradles. During the deployment, the *Harry S. Truman*'s crew rarely deployed the TWS array.
- In July 2016, the Navy, in conjunction with the TWS and CAT system contractors, conducted contractor testing of both the TWS and CAT on the Nanoose Bay, British Columbia, Canada, acoustic tracking range. The Navy installed a roll-on/roll-off version of the TWS and CAT system aboard the USNS *Brittin*, which served as a deep draft test platform. The TWS array consisted of the passive array (similar to the array deployed on carriers) and the latest version of the active source (TAAS). The testing included structured scenarios requiring a TWS system and operator to detect/alert on threat torpedoes, initiate a CAT salvo engagement, and for the CATs to intercept the threat torpedoes. Test scenarios also assessed TWS alert and false alert rates; TWS and CAT interoperability; TAAS and passive array reliability; and TWS array speed, turn rate, depth, and stability tow profiles. The Navy recorded the TWS and CAT data during all events for later analysis and reprocessing in future versions of the system.

Assessment

- The combined TWS and CAT contractor testing in July 2016 demonstrated the Navy's contractors are making progress toward developing an initial defensive capability to counter a salvo of threat torpedoes.
  - The testing demonstrated the TWS active and passive system, with a highly qualified sensor operator, is capable of detecting, tracking, and alerting on threat torpedoes, that operators can initiate a salvo of CATs to intercept the threat torpedoes, and that a salvo of CATs can intercept a salvo of threat torpedoes.
  - However, to achieve the test objectives, the contractor test scenarios were highly structured, were not conducted with realistic threat torpedo profiles, and were not conducted in conjunction with events that could have provided potential false alerts.
  - Safety considerations, implemented to prevent a collision between the threat torpedo surrogates, the CATs, and the deep draft tow ship, also prevented assessing the TWS detection capability for threats that operate near the surface. The same limitations prevent assessing the CAT's ability to detect, track, and intercept threat torpedoes in this challenging region of the water column.
  - Testing and data collection near the surface is necessary for developing the torpedo defense capability and this testing could be accomplished safely in a controlled manner without a deep draft tow ship.
- The July 2016 contractor testing demonstrated the Navy's TWS array contractors are making progress towards implementing solutions for the passive array twisting problem and with fixing the TAAS reliability failure modes. The July test event completed with no TWS or CAT hardware failures. This included 64 hours of TAAS active operations, 14 array deployments and retrievals, and 11 CAT or Electric-drive CAT (ECAT) launches.
- Completed testing also demonstrated the importance of having a trained TWS operator to initiate manual threat alerts when the automated detects and alerts are not initiated or occur late for assessing if threat alerts are valid or false.
- The testing of TWS (passive) and CAT EDM-2, powered by SCEPS, fielded aboard *George H. W. Bush*, *Theodore Roosevelt*, *Harry S Truman*, and *Dwight D. Eisenhower* has yet to demonstrate an effective capability against realistic threat torpedo attack scenarios.
  - The Navy's testing of the fielded TWS system has shown it is capable of detecting and targeting a threat torpedo and CAT demonstrated the limited capability to detect and home on certain types of torpedo threats. However, this capability assessment is based on limited testing conducted in areas with generally benign acoustic conditions when compared to the expected threat operating areas, which may bias the results high.
  - Very few of the threat surrogates used during testing were operated in operationally realistic threat torpedo profiles due to Navy-imposed safety constraints. Additionally, the acoustic properties of the current surrogate torpedoes are suspected to be louder than most threats in certain operating circumstances.
- The program's focus on preparing systems to deploy on carriers has hampered their development of more extensive system detection; tracking and alerting software; operator tactics, techniques, and procedures; and assessments of system availability and reliability because of their limited budget. Although the Pennsylvania State University Applied Research Laboratory was able to conduct independent structured CAT testing, 3Phoenix's TWS testing is limited because the prototype TWS arrays are rapidly fielded to the deploying CVN, leaving the 3Phoenix contractors without a full system to continue development. The Navy hoped to obtain data from the deployed CVNs to support TWS development, but their operations did not permit that. The July 2016 testing, which utilized portions of the systems removed from carriers following their deployments, provided a significant amount of recorded data (subject to the limitations discussed above) to support continued contractor development of the TWS and CAT systems.
- The Navy delayed the Initial Operational Capability of the TWS and CAT from 2018 to 2022. Because the Navy required the Program Office to deliver an early capability for the early fielded TWS and CAT, it has resulted in a 3- to 4-year delay in delivering the Capability Development Document-required torpedo defense capability to the CVNs.
- The Navy's decision to add a highly-trained contractor as the acoustic operator to supplement the automated detection and alerting functions of TWS has improved threat detection performance during all completed test events. DOT&E assesses the majority of the TWS's detection and alerting capability is a result of the contractor acoustic operators monitoring the TWS displays to provide early alerts on threat torpedoes. However, the test areas did not offer the same number of opportunities for false alerts as expected in the threat area; thus, it is not known if the presence of the operator could also reduce the false alarm rate. For safety reasons, testing was highly structured, which allowed the operators to focus on torpedo detections and firing the CAT. Therefore, completed testing was inadequate to resolve the rate of false alarms or their effect on mission accomplishment.
- Additional information concerning the testing of the fielded TWS and CAT performance is included in DOT&E's March 2015 classified Early Fielding Report.

Recommendations

- Status of Previous Recommendations. The Navy has made some progress on previous recommendations. However, the Navy should still:
  1. Complete the TEMP for the TWS and CAT system and an LFT&E strategy for the ATT lethality as soon as possible.
  2. Conduct additional testing in challenging, threat representative environments.
  3. Conduct additional CAT testing using operationally realistic threat target profiles closer to the surface to assess

the CAT's terminal homing, attack, and fuzing within the lethality range of the warhead.
4. Investigate test methods designed to reduce or eliminate the safety limitations that have previously prevented testing against operationally realistic target scenarios. The Navy should consider using geographic separation, range boundaries, and shallow draft ships for future TWS and CAT testing.
5. Continue to investigate, correct, and retest deficiencies identified with the active source before planning to field TAAS.
6. Adequately resource the TWS program to build dedicated test assets and conduct adequate dedicated contractor and developmental testing.
7. Adequately resource the Program Office and its contractors to conduct TWS and CAT system development and testing.
8. Investigate and implement the outstanding recommendations in the classified March 2015 DOT&E Early Fielding Report.

- FY16 Recommendation.
  1. The Navy should measure the signatures of available surrogates at representative threat torpedo depths and speeds. The Navy should also determine the adequacy of available torpedo surrogates to represent threat torpedoes.

Tactical Tomahawk Missile and Weapon System

Executive Summary

- The FOT&E Operational Test Launch program concluded in 2013. That phase of operational testing ran from 2004 to 2013. Upon completion of the Operational Test Launch program, DOT&E removed the Tomahawk Weapon System (TWS) from operational testing oversight. This decision was based upon TWS' history of consistent satisfactory performance over the past 9 years in test planning, test execution, and meeting reliability and performance requirements.
- Flight testing to evaluate All-Up Round changes, emerging deficiencies requiring immediate correction, and hardware obsolescence continued under a program monitored by the Navy's Commander, Operational Test and Evaluation Force.
- In 2016, Tactical Tomahawk Weapon Control System (TTWCS) operational test event OT-D-8 included cybersecurity events, a reliability/maintainability maintenance demonstration, non-firing strike group scenario, and modeling and simulation flight test events. OT-D-8 is planned to conclude in FY17 with a live fire flight test. As the program was not under T&E oversight, DOT&E did not oversee these test events or approve the test plan.
- In 2016, the Navy started development of an acquisition strategy for a series of incremental upgrades that modify the Block IV Tactical Tomahawk (TACTOM) into a Maritime Strike Tomahawk (MST) to develop an anti-ship capability. Consistent with mission changes brought about by plans to develop an anti-ship capability, the TWS was placed back on DOT&E oversight. The Navy intends to field MST as a Rapid Deployment Capability (RDC) with a Quick Reaction Assessment (QRA) test strategy. DOT&E assessed that the QRA would not support an adequate operational test but the Navy continues to not plan for any additional operational testing.
- To collect sufficient data for an adequate assessment of the capability, DOT&E identified the need for 36 test flights (based on the existing validated requirements for the Offensive Anti-Surface Warfare (OASuW) program since there were no identified requirements for MST), which could be accommodated by a combination of developmental and operational tests. This test scope could be reduced if the program undertakes an effort to develop a tactical software-in-the-loop modeling and simulation test bed similar to the current Tomahawk modeling and simulation test bed for the land attack mission area.
- The Navy has yet to provide any plans required to assess the functionality and lethality of the warhead against the new MST target set.

System

- The Tomahawk Land Attack Missile is a long-range, land attack cruise missile designed for launch from submarines and surface ships. Beginning in 2017, the Navy plans to develop the MST anti-ship capability as part of the Block IV modernization program.
- There are three fielded variants: a Block III with a conventional unitary warhead, a Block III with a conventional submunitions warhead, and a Block IV with a conventional unitary warhead. Production of Tomahawk Block II and III missiles is complete. Block IV Tomahawk is in production as the follow-on to the Block III conventional unitary warhead variant. These missiles are produced at lower cost and provide added capability, including the ability to communicate and be redirected to an alternate target during flight.
- The Tomahawk Weapon System (TWS) also includes the Tomahawk Theater Mission Planning Center (TMPC) and the shipboard TTWCS. The TMPC and TTWCS provide for command and control, targeting, mission planning, distribution of Tomahawk tactical and strike data, and post-launch control of Block IV missiles.

Mission

The Joint Force Commander employs naval units equipped with the TWS for long-range, precision strikes against land targets. Planned upgrades will allow the Joint Force Command to employ the TWS in anti-ship missions.

Major Contractors

- Missile element: Raytheon Missile Systems – Tucson, Arizona

- Weapon Control System element: Lockheed Martin – Valley Forge, Pennsylvania
- Mission Planning Element:
  - Vencore, Inc. – San Jose, California (Mission Distribution System)
  - Tapestry Solutions – St. Louis, Missouri (Tomahawk Planning System)
  - BAE Systems – San Diego, California (Targeting Navigation Toolset)

Activity

- In 2013, DOT&E removed the TWS from operational testing oversight. This decision was based upon TWS's history of consistent satisfactory performance over the past 9 years in test planning, test execution, and in meeting reliability and performance requirements. Flight testing to evaluate All-Up Round changes, emerging deficiencies requiring immediate correction, and hardware obsolescence continued under a program monitored by the Navy's Commander, Operational Test and Evaluation Force.
- In 2016, based on direction by the Deputy Secretary of Defense, the Navy started development of an acquisition strategy for a series of incremental upgrades that modify the Block IV TACTOM into an MST. The Navy plans to insert this capability in a subset of the TACTOM population (Block IV) as these missiles are inducted into the recertification line.
- In 2016, operational test event OT-D-8, that commenced while the program was not under DOT&E oversight, continued. Testing included cybersecurity events, a reliability/maintainability maintenance demonstration, non-firing strike group scenarios, and modeling and simulation flight test events. OT-D-8 is planned to conclude in FY17 with a live fire flight test. As the program was not under T&E oversight, DOT&E did not oversee these test events or approve the test plan.

Assessment

- The Navy plans to insert the MST capability into the Block IV TACTOM missiles as they go through their modernization process (potentially up to 4,000 rounds), which is a de-facto full fielding of the new mission enhancement. Currently, the Navy does not intend to develop an MST Capability Development Document/Capability Production Document or any other type of requirements document to guide the developmental or operational test planning. Rather, the Navy will issue a "Capability Memorandum." The form and utility of this document for acquisition and test planning purposes remains undetermined.
- The Navy intends to field MST as an RDC supported by a QRA test. Despite being advised by DOT&E that the QRA would not be an adequate operational and live fire test, the Navy continues to not plan for any additional operational and live fire tests. Traditionally, RDCs conduct QRAs in order to support a decision to expeditiously field an initial capability but then plan a full operational test program to support their full-fielding decision. Plans to conduct operational or live fire testing to support the capability deployment are unclear because there are no scheduled Milestones for the TACTOM program.
- DOT&E provided the Navy with an initial operational test design based on the existing validated requirements for the OASuW program as there were no identified requirements for MST. While the OASuW material solution is different (Long Range Anti-Ship Missile (AGM-158C LRASM)), the basic mission was assumed to be similar enough to develop a test design. To collect sufficient data for an adequate assessment of the capability, the test design identified the need for 36 test flights between developmental and operational testing. This number could be reduced if the program undertakes an effort to develop a tactical software-in-the-loop modeling and simulation test bed similar to the current Tomahawk modeling and simulation test bed for the land attack mission area. Because of the very different environments and target characteristics, the current modeling and simulation test bed, optimized for the land attack mission, is not adequate for the maritime strike mission.
- The Navy has yet to provide any plans needed to rigorously assess the functionality and lethality of the warhead against the new MST target set.

Recommendations

- Status of Previous Recommendations. The Navy has addressed all previous recommendations.
- FY16 Recommendations. The Navy should:
  1. Develop and validate operational requirements for the MST mission.
  2. Plan to conduct, and budget appropriately for, full operational and live fire testing of the MST capability. This should include development of a tactical software-in-the-loop modeling and simulation test bed, and functionality and lethality testing of the warhead for the new target set.

VH-92A Presidential Helicopter Replacement Program

Executive Summary

- The VH-92A program is progressing on or ahead of schedule.
- The VH-92A system-level Critical Design Review was held July 18 – 21, 2016, and resulted in minimal action items, which are all progressing to closure.
- Modifications to two Sikorsky S-92A aircraft to produce two VH-92A aircraft continue on schedule with modification completion projected in FY17. This effort includes the Lockheed Martin integration of the Mission Communications System (MCS) designed by Naval Air Systems Command (NAVAIR) at St. Inigoes, Maryland.
- Contractor flight testing is projected to commence in mid-FY17.
- VH-92A-unique fuel bladders did not pass drop tests and mitigation efforts are ongoing. The program intends to qualify the bladders for flight partially full so flight tests will not be delayed.
- There are some challenges relative to connection to the Crisis Management System and the Executive Airlift Command Network. Work on solving these challenges is ongoing.

System

- The VH-92A aircraft will replace the current Marine Corps fleet of VH-3D and VH-60N helicopters flown by Marine Helicopter Squadron One to perform the presidential airlift mission.
- The VH-92A is a dual-piloted, twin-engine helicopter based on the Sikorsky S-92A. The Navy intends the VH-92A to maintain Federal Aviation Administration (FAA) airworthiness certification throughout its lifecycle.
- The VH-92A is planned to be capable of operating worldwide in day, night, or adverse weather conditions. The VH-92A will be air-transportable to remote locations via Air Force C-17 cargo aircraft.
- The government-designed MCS will provide the ability to conduct simultaneous short- and long-range secure and non-secure voice and data communications. It can exchange situational awareness information with outside agencies, organizations, and supporting aircraft. The MCS will be integrated into the VH-92A by Lockheed Martin in Owego, New York.
- Delivery of the first two Engineering Development Models (EDM-1 and EDM-2) is planned for 2018, followed by four System Development Test Article aircraft in 2019.

Mission

- Marine Helicopter Squadron One equipped with the VH-92A aircraft will provide safe and timely transport of the President of the United States and other parties as directed by the White House Military Office.
- The VH-92A is required to operate from commercial airports, military airfields, Navy ships, and austere sites throughout the world.

Major Contractors

- Sikorsky Aircraft Corporation (owned by Lockheed Martin since November 2015) – Stratford, Connecticut
- Lockheed Martin – Owego, New York

Activity

- The VH-92A program completed co-site risk reduction tests in September 2015 using a Sikorsky S-92A modified with antennas planned for the VH-92A configuration. Tests on this aircraft (designated at the time as EDM-0) provided data that led to refinement of the VH-92A design early in the program.
- Modifications to EDM-0 and a second S-92A aircraft into EDM-1 and EDM-2 (the VH-92A configuration) are on schedule.
- NAVAIR at St. Inigoes is designing the MCS software. NAVAIR has delivered MCS hardware and initial software to Lockheed at Owego for EDM-1 and EDM-2. Lockheed Martin is integrating the MCS into the VH-92A system architecture and is assembling installation kits for each aircraft.
- Systems integration laboratories, which replicate the MCS for development, test, and training, are up and running and MCS software development is on schedule.

- The VH-92A System Critical Design Review was held July 18 – 21, 2016. All requests for action and information are resolvable to bring the Critical Design Review to closure.
- The VH-92A-unique fuel bladders failed during drop testing. Mitigation efforts are progressing with the assistance of NAVAIR experts and Sikorsky engineers. In order to maintain FAA certification and not delay flight testing, the bladders will initially be qualified at a reduced fuel level.
- Live fire testing is proceeding well without major concerns.

Assessment

- The program is progressing on or ahead of schedule. Maintenance of FAA airworthiness certification is a key emphasis area.
- Lockheed Martin is on schedule to deliver MCS kits for EDM-1 and EDM-2 in 1QFY17.
- Sikorsky is on schedule to complete modification/manufacture of EDM-1 and EDM-2 in FY17.
- Contractor testing is projected to commence in mid-FY17.
- Delivery of EDM-1 and EDM-2 is projected for FY18 followed by the commencement of integrated testing.
- An operational assessment is planned for 4QFY18 to support a Milestone C decision in 2QFY19. A two-aircraft operational assessment is planned for 30 flight hours over 30 days using HMX-1 aircrews. The Commander, Operational Test and Evaluation Force (COTF) will function as the Operational Test Agency and testing will be overseen by COTF and DOT&E. Timing of EDM-2 delivery in time for this operational assessment is a watch item.
- Fuel bladder deficiencies are being appropriately addressed and are expected to be resolved in the near future.
- The program is facing some challenges meeting the Net Ready Key Performance Parameter for the MCS relative to connection to the Crisis Management System and connection to the Executive Airlift Command Network. Work is continuing on resolving these integration issues.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The program should:
  1. Complete mitigation efforts for fuel bladders.
  2. Complete plans for the operational assessment planned for 4QFY18.
  3. Continue planning efforts for HMX-1 transition to VH-92A.

Air Force Programs

Air Force Programs

AC-130J Ghostrider

Executive Summary

- U.S. Special Operations Command (USSOCOM) is developing AC-130J through the integration of a modular Precision Strike Package (PSP) onto existing MC-130J aircraft. An earlier version of the PSP was previously developed and tested on several AC-130W aircraft since 2009 and fielded in 2010.
- The 18th Flight Test Squadron conducted an Operational Utility Evaluation (OUE) of the Block 10 AC-130J from December 2015 to March 2016 to support Milestone C and an early fielding decision, but USSOCOM will not pursue early fielding of Block 10.
- The Block 10 PSP demonstrated system immaturity during the OUE that diminished the usability of the system. The AC-130J entered operational testing with numerous open deficiency reports (DRs), which required aircrews to use burdensome workarounds in order to conduct their missions. Almost none of the surveyed aircrew rated the system "usable" during the OUE.
- In single-weapon live-fire engagements during the OUE, the AC-130J successfully achieved nominal direct hits and effective kills against two static and two moving targets with Griffin missiles and four static targets with Small Diameter Bombs (SDBs) using two different target coordinate systems.
- The OUE discovered problems with the 30 mm gun control system that affected its accuracy. Preliminary results from an upgraded gun tuning software resident in Block 20 indicate both the 105 mm and 30 mm guns are performing within accuracy specifications.
  - Preliminary results from lethality analysis of the PGU-46/B 30 mm round against mannequin targets indicate that this round has limited effectiveness against personnel in the open on soft ground but is more effective against personnel on hard surfaces.
  - Data also indicate that lethality to personnel above a "soft" plywood roof is lower than predicted by existing models because the round detonated below the roof's surface; mannequins above a concrete roof incurred more fragmentation damage than above a plywood roof.
- Cybersecurity testing of the Block 10 PSP found vulnerabilities that are described in the classified Cooperative Vulnerability and Penetration Assessment (CVPA) report. These vulnerabilities are addressed in Block 20 software modifications.
- Lockheed Martin delivered the first Block 20 AC-130J to USSOCOM in July 2016 to begin developmental testing of new capabilities, such as the 105 mm gun. As of the end of FY16, the program received eight donor MC-130J for modification and produced four AC-130J. The first AC-130J, which experienced a Class A mishap in FY15 rendering it

non-flyable, will become an Air Education and Training Command training asset.
- The 18th Flight Test Squadron will conduct IOT&E on a Block 20 aircraft from March through June 2017 to support a Full-Rate Production decision in 1QFY18.

System

- The AC-130J is a medium-sized, multi-engine, tactical aircraft with a variety of sensors and weapons for air-to-ground attack.
- USSOCOM is developing the AC-130J by integrating a modular PSP onto existing MC-130J aircraft, and replacing the MC-130J refueling pods with weapon racks. USSOCOM continues to develop new PSP capabilities on legacy AC-130W aircraft in parallel before they are introduced on the AC-130J in an evolutionary acquisition approach:
  - The Block 10 AC-130J PSP provides a weapons suite that includes an internal, pallet-mounted 30 mm side firing chain gun; wing-mounted, GPS-guided SDBs; and Griffin laser-guided missiles mounted internally and launched through the rear cargo door.
  - The PSP also provides two electro-optical/infrared sensor/laser designator pods and multiple video, data, and communication links.
  - A dual-console Mission Operator Pallet (MOP) in the cargo bay controls all PSP subsystems with remote displays and control panels (including master arm and consent switches and a gun trigger) on the flight deck. An interim, limited-functionality, carry-on flight deck workstation for a Combat Systems Officer has been added to the Block 10 AC-130J.
  - Block 20 AC-130J adds a 105 mm gun, laser-guided SDB, a side-mounted pilot tactical display, and Large Aircraft Infrared Countermeasures. The aircrew will increase

from seven to nine. The first Block 20 configuration was delivered on aircraft number 4 in July 2016.
  - Future updates are expected to include a permanent Combat Systems Officer station, wing-mounted HELLFIRE missiles, radio-frequency countermeasures (RFCM), all-weather engagement capability, and on a limited number of aircraft, a high-energy laser.
- The AC-130J retains all survivability enhancement features found on the MC-130J aircraft.
  - Susceptibility reduction features include the AN/ALR-56M radar warning receiver, the AN/AAR-47(V)2 missile warning system, and the AN/ALE 47 countermeasure dispensing system.
  - Vulnerability reduction features include fuel system protection (fuel tank foam to protect from ullage explosion), redundant flight-critical components, and armor to protect the crew and the oxygen supply.
- The AC-130J will replace legacy AC-130H/U aircraft.

Mission

The Joint Task Force or Combatant Commander will employ units equipped with the AC-130J to provide close air support and air interdiction using battlespace wide area surveillance, target geolocation, and precision munition application.

Major Contractor

Lockheed Martin – Bethesda, Maryland

Activity

- The 18th Flight Test Squadron conducted an OUE in accordance with the DOT&E-approved test plan of the Block 10 AC-130J from December 2015 to March 2016 to support an early fielding decision. USSOCOM has subsequently decided not to pursue early fielding of Block 10. Testing consisted of 18 sorties and 74 flight hours during the dedicated OUE period and accomplished approximately half of the operational test designs for the Griffin missile and the SDB. The remainder of the Griffin and SDB tests will occur in IOT&E.
- The OUE included cooperative cybersecurity testing of most of the PSP, but precision-guided munition subsystems and aircraft avionics and support systems were not part of the test, and DOT&E did not approve the cybersecurity test plan. The Block 20 AC-130J will undergo a full-aircraft CVPA and an Adversarial Assessment during IOT&E.
- Live fire tests during the OUE and follow-on developmental testing comprised the first phase of AC-130J weapons effectiveness testing. The 780th Test Squadron collected live fire data against operationally representative mannequin and vehicle targets to support lethality evaluation of the 30 mm gun and the Griffin missile. Block 20 testing will include additional Griffin engagements and characterization of the 105 mm gun.
- Lockheed Martin delivered the first Block 20 AC-130J to USSOCOM in July 2016 to begin developmental testing of new capabilities, such as the 105 mm gun. As of the end of FY16, the program received eight donor MC-130J for modification and produced four AC 130J. The first Block 10 AC 130J, which experienced a Class A mishap in FY15 rendering it non-flyable, will become an Air Education and Training Command training asset.
- Block 20 developmental testing began in July and includes additional flying and handling qualities tests to verify flight characteristics of the modified aircraft are consistent with technical data. The program expects to complete developmental testing in December 2016.
- Through a Memorandum of Agreement, USSOCOM Program Executive Office-Fixed Wing, Air Force Special Operations Air Warfare Center, 96th Test Wing, and 1st Special Operations Wing formed a Special Operations Combined Test Force to conduct AC-130J developmental testing in lieu of the traditional Air Force Materiel Command framework. Test team members and aircrew will come from 1st Special Operations Wing (1st Special Operations Group Detachment 2), 96th Test Wing (413th Flight Test Squadron), and Air Force Special Operations Air Warfare Center (18th Flight Test Squadron), depending on the nature of the test sortie.
- The Program Office submitted, and DOT&E approved, an updated Test and Evaluation Master Plan (TEMP) in July to support a Milestone C decision in September. The program updated the TEMP to include full-aircraft cybersecurity testing and phase two lethality testing of the Griffin missile and 105 mm gun as part of developmental and operational testing of the Block 20 AC-130J.
- The 18th Flight Test Squadron will conduct IOT&E on a Block 20 aircraft from March through June 2017 to support a Full-Rate Production decision in 1QFY18. IOT&E will complete the Griffin and SDB tests, add 105 mm gun and Laser Small Diameter Bomb (LSDB) testing, and repeat much of the 30 mm gun testing due to problems discovered in the OUE.
- The 780th Test Squadron, in coordination with DOT&E, has submitted the phase two weapons lethality test plan for the Griffin missile and 105 mm gun to the Combined Test Force for approval and execution. The plan includes four more Griffin missile engagements against static ground and maneuvering boat targets and 105 mm gun engagements against structures, personnel, technical vehicles, and lightly armored air defense vehicles.
- USSOCOM is developing an RFCM system for MC-130J and AC-130J under a separate Acquisition Category II program. A recent change in program strategy will implement and test

the system first on the AC-130J instead of the MC-130J, with RFCM IOT&E on an AC-130J scheduled for 4QFY18. The RFCM program plans a Milestone B decision and source selection in 1QFY17.
- The U.S. Air Force Combat Effectiveness and Vulnerability Analysis Branch expect to have completed the Ballistic Vulnerability Analysis, Anti-Aircraft Artillery Susceptibility Analysis, Proximity Burst Analysis, and Occupant Casualty Analysis by 2QFY17. These analyses are being conducted in accordance with the LFT&E Alternate Test Plan.

Assessment

- The Block 10 PSP demonstrated system immaturity during the OUE that diminished the usability of the system. The system entered operational testing with numerous open DRs, which required aircrews to use burdensome workarounds in order to conduct their missions. Almost none of the surveyed aircrew rated the system "usable" during the OUE.
  - The Block 10 AC-130J entered the OUE with 19 Category 1-Urgent and 60 Category 2-Urgent open DRs. Testing generated 10 additional Category 1-Urgent or Category 2-Urgent DRs. The program has since closed out 18 DRs, but only downgraded the severity of 6 Category 1-Urgent and 1 Category 2-Urgent DRs.
  - Nine Category 1-Urgent DRs remained open as of the OUE report covering the following problems:
    - MOP computers become overloaded and perform poorly or must be reset (two DRs).
    - Software does not update target coordinates frequently enough in some modes.
    - MOP hand controllers do not provide adequate control of the sensor or may allow accidental movement of the targeting sensor (two DRs).
    - Laser designator frequently does not fire, and settings may spontaneously change during editing (two DRs).
    - One of the aircraft radios interferes with the PSP GPS receiver.
    - Oxygen hoses are too short.
  - The Block 20 update is designed to address eight of the Category 1-Urgent DRs, which are currently under evaluation. The DR on GPS receiver interference remains open.
- The overall operating environment aboard the AC-130J also diminished PSP usability. Crews reported problems with night-vision goggle compatibility caused by MOP display screens, gun noise preventing hands-free communication on the intercom system, the temporary flight deck workstation laptop physically interfering with aircraft controls and displays, and a physically challenging aft-cabin environment due to the "roll-on" nature of the PSP creating multiple trip hazards and narrow passageways.
  - The test team submitted a Category 1-Urgent and a Category 2-Urgent DR regarding trip hazards in the cargo compartment where special mission aviators routinely carry high-explosive ammunition, but the material improvement project review board downgraded the Category 1-Urgent DR to Category 2-Urgent.
- Previously reported problems with the Block 10 PSP sensors appear to have been corrected as of the OUE and will be validated during IOT&E of Block 20. No un-commanded sensor movements occurred that were not attributable to allowing the sensor to pass through nadir.
- Block 10 flying and handling qualities testing showed no significant differences from basic C-130J performance as a result of the AC-130J modifications. An Air Force Materiel Command investigation into the Class A mishap on the first aircraft attributed the departure from controlled flight primarily to improper control inputs and test procedures.
- Although the OUE missions did not experience the same kind of complete shutdowns of MOP computers that crews observed during the operational assessment, operators still frequently reported software instability and poor computer performance during more complex tasks. Hardware and software upgrades on Block 20 MOP are intended to resolve these issues and will be evaluated during IOT&E.
- In single-weapon live-fire engagements during the OUE, the AC-130J successfully achieved nominal direct hits against two static and two moving targets with Griffin missiles and four static targets with SDBs using two different target coordinate systems.
  - Preliminary results from lethality analysis of the Griffin vehicle targets indicate mobility kills against a stationary truck and two moving trucks in both height-of-burst and point-detonate modes, which appear to correlate well with pre-test modeling and simulation; however, the level of incapacitation and effective distance of fragmentation against personnel appear to be lower than predicted by existing models.
- The OUE discovered problems with the 30 mm gun control system that affected its accuracy and are still under investigation. Preliminary results during Block 20 developmental testing indicate an upgraded gun tuning software has resolved the DR and both the 105 mm and 30 mm guns are performing within accuracy specifications.
  - Preliminary results from lethality analysis of the PGU-46/B 30 mm round against mannequin targets indicate that this round has limited effectiveness against personnel in the open on soft ground but is more effective against personnel on hard surfaces.
  - Data also indicate that lethality to personnel above a "soft" plywood roof is lower than predicted by existing models because the round detonated below the roof's surface; mannequins above a concrete roof incur more fragmentation damage than above a plywood roof.
  - USSOCOM has indicated that it may change the standard operational round for the 30 mm gun from PGU-46/B to PGU-13D/B for production reasons. If the operational round changes, the program will need to repeat the phase one lethality testing with the new round to characterize

its effectiveness in the LFT&E report required for the Full-Rate Production decision.

- The OUE did not adequately support DOT&E evaluation of the suitability of crew compartment armor because the crews did not install it during test flights for weight and balance reasons that will be remedied by the addition of the 105 mm gun in the rear of the aircraft. However, a ground demonstration indicates that crew compartment armor hinders crew egress in an emergency.
- Cybersecurity testing of the Block 10 PSP found vulnerabilities that are described in the classified CVPA report. The program expects to test and verify remediation of these deficiencies in April 2017 as part of the Block 20 CVPA.
- The mission success-based measure of Weapon System Reliability exceeded the Capabilities Production Document requirement of 82 percent during the OUE, but the AC-130J experienced hardware and software failures that diminished system effectiveness and limit the system's inherent availability.
- The AC-130J still does not satisfy two Key System Attributes from the Capabilities Production Document:
  - The program has not implemented a solution to provide flight deck crew a geo-rectified tactical display superimposed on the field of view. A side-mounted heads-up display next to the pilot station is planned for Block 20 and is expected in early FY17, but it is not yet available for developmental testing to ensure its readiness for IOT&E.
  - The AC-130J does not have a sensor system that enables adverse weather engagements by detecting and tracking targets obscured by weather, smoke and haze, or obscurants. Earlier efforts to integrate an AN/ASQ-236 radar pod were unsuccessful.
- The current test schedule leaves only 29 days between delivery of the developmental test and evaluation report and the start of IOT&E, with an operational test readiness review 22 days before IOT&E instead of the recommended 45 days. This raises the risk that any problem discoveries in developmental testing may delay the start of IOT&E or adversely affect the evaluation of the AC-130J.

Recommendations

- Status of Previous Recommendations.
  1. The program included the recommended lethality testing in the TEMP update for Milestone C, has conducted phase one lethality testing of the Griffin and 30 mm gun, and plans to conduct phase two lethality testing prior to IOT&E. However, a change in ammunition for the 30 mm gun will require a repeat of that portion of testing.
  2. The program briefed an updated baseline for block capability development and fielding at the June 2016 program management review, but it is not reflected in the Milestone C TEMP, and the test strategy for the new capability increments is unclear.
- FY16 Recommendations. The Program Office should:
  1. Correct, close, and verify all Category 1-Urgent DRs and as many Category 2-Urgent DRs as possible prior to IOT&E.
  2. Conduct additional 30 mm lethality testing using PGU-13D/B in time to support the Full-Rate Production decision if that round is likely to be employed in combat.
  3. Include a clear test strategy for future testing of the new capability increment baseline in the TEMP update for the Full-Rate Production decision.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

Executive Summary

- The Air Force and Navy completed FOT&E of the AIM-120D Advanced Medium-Range Air-to-Air Missile (AMRAAM) in July 2014 and fielded the system in January 2015.
- The Services completed operational test activities for the AIM-120D System Improvement Program (SIP)-1 in FY16. The results are pending. SIP-1 is one of several follow-on programs designed to enhance AIM-120D performance.
- The Services completed operational test activities for the AIM-120 AMRAAM Basic Electronic Protection Improvement Program (EPIP), a software upgrade to AIM-120C3-C7 variants, in FY16. Basic EPIP met its requirements.
- The Services began operational test activities for the AIM-120 AMRAAM Advanced EPIP, a software upgrade to the AMRAAM C-7 variant, in FY16.
- The Air Force and Navy are in the final stages of test planning to conduct cybersecurity testing for all variants of the AMRAAM missile.

System

- AMRAAM is a radar-guided, air-to-air missile with capability in both the beyond visual-range and within visual-range arenas. A single-launch aircraft can engage multiple targets with multiple missiles simultaneously when using AMRAAM.
- F-15C/D/E, F-16C/D, F/A-18C/D/E/F, EA-18G, and F-22A aircraft are capable of employing the AMRAAM, and the missile is currently being tested/fielded for employment on the F-35A/B/C.
- The AMRAAM program periodically develops and incorporates phased upgrades. The AMRAAM Basic EPIP is a software upgrade to AIM-120C3-C7. An Advanced EPIP software upgrade began operational testing in FY16.

Mission

- The Air Force and Navy, as well as several foreign military forces, employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions.
- All U.S. fighter aircraft use the AMRAAM as the primary, beyond visual-range air-to-air weapon.

Major Contractors

- Raytheon Missile Systems – Tucson, Arizona
- Rocket Motor Subcontractor: Nammo (Nordic Ammunition Group) – Raufoss, Norway

Activity

- The Air Force and Navy conducted all testing in accordance with DOT&E-approved test plans.

AIM-120D

- The Services completed SIP-1 testing in FY16. Assessment of effectiveness and suitability is pending.
- SIP-2 operational test planning is in progress. Testing is scheduled to begin in FY17 and finish in FY18.

AMRAAM EPIP

- The Services completed operational testing for the Basic EPIP software upgrade to C-3 through C-7 missiles in FY16.
- Operational testing for the Advanced EPIP software upgrade to C-7 missiles began in FY16 and is expected to complete in FY17.

Cybersecurity

- The Air Force and Navy are in the final stages of test planning to conduct cybersecurity testing for all variants of the AMRAAM missile.

Assessment

- AMRAAM continues to be operationally effective and suitable.
- Based on FY15 testing, the AIM-120D SIP-1 missile appears to be meeting performance and reliability requirements, although a final assessment is pending.
- Missiles equipped with Basic EPIP software are meeting performance requirements.

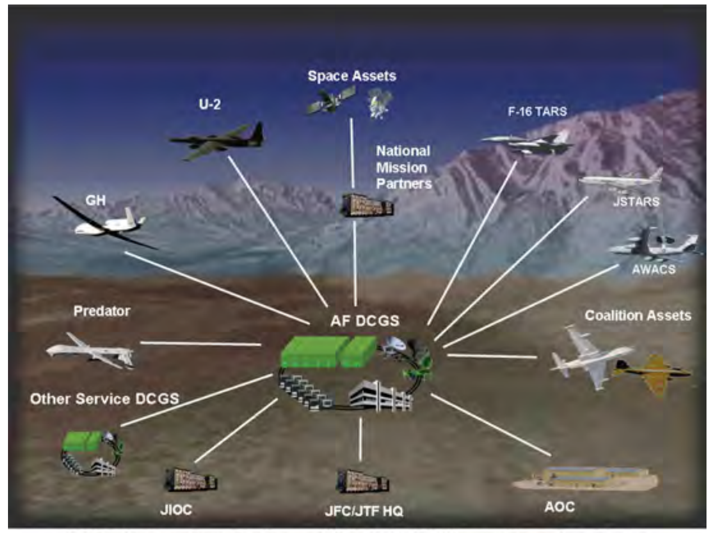
Recommendations

- Status of Previous Recommendations. Although test planning and execution are ongoing, the Air Force has not yet satisfactorily addressed the previous FY15 recommendations to:
  - Complete SIP-2 and Advanced EPIP operational testing to achieve the Services' desired mission effectiveness improvements for AMRAAM.
  - Complete cybersecurity testing for all variants of the AMRAAM missile in accordance with the August 1, 2014, DOT&E policy memorandum.
- FY16 Recommendations. None.

Air Force Distributed Common Ground System (AF DCGS)

Executive Summary

- The Air Force Distributed Common Ground System (AF DCGS) consists of eight Acquisition Category (ACAT) III programs. The Air Force plans to phase out the current architecture and move toward an open architecture. The Air Force is updating test and evaluation, systems engineering, and requirements documentation based on the open architecture.
- The Air Force Operational Test and Evaluation Center completed an Operational Utility Evaluation (OUE) of System Release (SR) 3.0 in September 2015. The test showed that the overall signal intelligence (SIGINT) performance is poor, and SR 3.0 did not significantly improve SIGINT performance. SR 3.0 is neither operationally suitable nor survivable against cyber threats.
- The Air Force 605th Test and Evaluation Squadron (TES) completed the second and third phases of the three-phased Force Development Evaluation (FDE) on the Geospatial Intelligence (GEOINT) Baseline (GB) 4.1 in November 2015 and April 2016, respectively. GB 4.1 added the ability to ingest new synthetic aperture radar data from Global Hawk Block 40. However, GB 4.1 did not significantly improve the Air Force GEOINT capabilities.



AOC - Air Operations Center
AWACS - Airborne Warning and Control System
GH - Global Hawk
HQ - Headquarters
JFC - Joint Forces Command
JIOC - Joint Intelligence Operations Center
JSTARS - Joint Surveillance Target Attack Radar System
JTF - Joint Task Force
TARS - Tactical/Theater Airborne Reconnaissance System

System

- The AF DCGS, also referred to as the AN/GSQ-272 SENTINEL weapon system, is an intelligence enterprise system that is composed of 27 geographically separated, networked sites, including 5 core sites across the globe.
- AF DCGS provides hardware and software tools for planning and direction, collection, processing and exploitation, analysis and dissemination (PCPAD) of intelligence, surveillance, and reconnaissance (ISR) information. The DCGS Integration Backbone provides the framework that allows sharing of ISR information with other military Services and intelligence agencies.
- The Air Force declared AF DCGS to be at Full Operational Capability in 2009 despite Air Force plans to continue system development.
- Currently, AF DCGS consists of eight ACAT III programs: Sensor Integration, GEOINT Transformation, GB 4.1, SIGINT Transformation, SR 3.0, Infrastructure Transformation, Multi-Intelligence, and DCGS Reference Imagery Transition (DRT).
- To date, only two of the eight programs have undergone operational testing: GB 4.1 and SR 3.0.
  - GB 4.1 is a GEOINT upgrade that includes deficiency corrections and the capability to process and exploit feeds from updated sensors such as the Airborne Cueing and Exploitation System – Hyperspectral. The GB 4.1 update also allows continued interoperability with the sensors on the Global Hawk Block 40.
  - SR 3.0 is a SIGINT upgrade, which makes SIGINT data and services available to internal and external users, improves operations with the Airborne Signals Intelligence Payload low-band sensor, and improves processing, exploitation, and dissemination for high-band sensors.
- The Air Force is in the process of transitioning AF DCGS to an open architecture system via an agile acquisition strategy. This transition is expected to take several years. The open architecture is designed to enable the Air Force to field modular upgrades and updates on a standardized infrastructure.

Mission

- The Air Force uses AF DCGS to plan sensor information requests and to produce intelligence information from data collected by a variety of sensors on the U-2, RQ-4 Global Hawk, MQ-1 Predator, MQ-9 Reaper, MC-12, and other ISR platforms.
- The Air Force uses AF DCGS to connect to the multi-Service DCGS Integration Backbone, manage requests for sensors, process sensor data, exploit sensor data from multiple sources, and disseminate intelligence products.

Major Contractors

- Raytheon – Garland, Texas
- Lockheed Martin – Denver, Colorado
- L-3 Communications – Greenville, Texas

Activity

- The Air Force Operational Test and Evaluation Center conducted the SR 3.0 OUE from September 10 to November 6, 2015. Testing was conducted in accordance with a DOT&E-approved test plan. DOT&E published a report on the test results on July 20, 2016.
- The 605th TES conducted Phase 2 of the three-phased GB 4.1 FDE from November 11 – 20, 2015, at Distributed Ground System (DGS)-2 and Phase 3 at DGS-1 from April 19 – 28, 2016. DOT&E reported on the results of the first phase of the FDE on November 23, 2015. The FDE was conducted in accordance with a DOT&E-approved test plan.
- The 605th TES conducted a high altitude mission workflow comparison test between the GEOINT Workflow Enhancement (GWE) and the GB 4.1 baseline (legacy) at DGS-X from March 28 – 30, 2016, to assess differences in the workflow of geospatial analysts.
- The 605th TES conducted GWE OUE from August 7 – 16, 2016, at DGS-1.

Assessment

- The Air Force does not have a test plan that integrates the eight ACAT III programs that comprise AF DCGS. This approach makes it difficult to determine if AF DCGS, as a whole, supports mission success. DOT&E is working with the Air Force to integrate test events. The integrated evaluation plan will be documented in the TEMP.
- The program lacks rigorous and comprehensive software problem tracking and reporting procedures. The Air Force is working to develop and implement the software tracking and reporting process.
- AF DCGS continues to have challenges executing PCPAD of GEOINT.
  - GB 4.1 did not deliver significant new capabilities other than the ability to work with Global Hawk Block 40 sensors.
  - Full motion video continues to have problems with freezing and degraded images. Full motion video analysts continue to rely on software that is not a part of AF DCGS.
  - The 605th TES observed problems creating secondary image products (images with analyst's annotations) in the GB 3.0 system and these problems continue in GB 4.1. A GEOINT exploitation tool called Softcopy Exploitation Tool – Geospatial Exploitation Products (SOCET GXP) occasionally creates secondary image products with corrupted metadata and metadata fields. When this happens, operators have to completely rebuild the secondary image product.
  - GB 4.1 continues to have problems with mission planning. In Phase 3 of the GB 4.1 FDE, some mission sets were not compatible with the external tasking service, forcing operators to manually complete mission planning.
  - Training and documentation continues to be problematic. In Phase 2 of the GB 4.1 FDE, for instance, 50 percent of general system administrators reported that documentation did not support maintenance duties. The test team reported that operators were using old checklists and had not been trained on the GB 4.1 system upgrades.
  - DOT&E will evaluate the GEOINT capability using the data from the GB 4.1 FDE and GWE OUE.
- The SR 3.0 OUE showed that the overall SIGINT performance was poor. Only a small percentage of collectable SIGINT was accurately reported.
  - SR 3.0 processing and exploitation software did not add significant operational value to the onboard processing and exploitation provided by the Airborne Signals Intelligence Payload on Global Hawk.
  - SR 3.0 reliability, availability, and maintainability were poor and negatively affected performance; SR 3.0 availability was 33 percent versus the required 98 percent.
  - SR 3.0 is not survivable against cyber-attacks.
- The 46th Test Squadron conducted a cybersecurity assessment of AF DCGS GEOINT 4.1 at DGS-X March through June 2015 and reported vulnerabilities. The Air Force is working on completing the Plan of Actions and Milestones (POA&M) to mitigate the vulnerabilities. DOT&E will work with the Air Force to maintain an accurate and timely cybersecurity POA&M.

Recommendations

- Status of Previous Recommendations. The Air Force satisfactorily addressed, or made satisfactory process towards implementing, six of the nine previous recommendations. The three recommendations still pending are:
  1. Submit a Test and Evaluation Master Plan (TEMP) for DOT&E approval, which includes an accurate description of AF DCGS requirements, architecture, and interfaces sufficient to justify the test approach. The Program Office is making good progress, but the TEMP is not yet approved.
  2. Develop and implement a software change request process including tracking of software metrics for problems open and closed by severity and time.
  3. Document all known cyber vulnerabilities and plan for mitigation in a POA&M and track the progress.
- FY16 Recommendations. None.

Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The Air Operations Center – Weapon System (AOC-WS) 10.1 is a system of systems that incorporates third-party software applications, to enable its mission execution.
- In October and November 2015, the Air Force conducted an assessment of Out-of-Cycle (OOC) 13.1 at Combined Air Operations Center – Experimental (CAOC-X).
  - OOC 13.1 was found to be not operationally effective due to three Category I deficiencies.
  - Resolution of the Category I deficiencies was scheduled to be accomplished in OOC 13.3 in November and December 2016; however, the Defense Information Systems Agency (DISA) failed to provide the Program Management Office with viable updates.
  - OOC 13.1 was found to be operationally suitable, and there were no significant cybersecurity findings.
  - The AOC Configuration Review Board (CRB) has recommended fielding OOC 13.1 despite the Category I deficiencies in order to meet other warfighter capability requirements.
- In February 2016, the Air Force conducted an assessment of OOC 13.2 at CAOC-X.
  - OOC 13.2 was found to be operationally effective and suitable, but one portion of software content introduced four Category II cybersecurity deficiencies. The Air Force removed the non-secure content from the delivery, deferring fielding until the four deficiencies are resolved.
  - The CRB approved fielding of OOC 13.2 in conjunction with the fielding of OOC 13.1, since its implementation requires a successful OOC 13.1 installation.
- AOC-WS 10.2 failed to complete a second round of developmental testing and the associated operational assessment activities.
  - The test was canceled at the half-way point due to the number and severity of deficiencies identified.
  - The program is now proceeding through a Critical Change Review.

System

- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that incorporates numerous software applications developed by third-party vendors and commercial off-the-shelf products. Each third party system integrated into the AOC-WS provides its own programmatic documentation.
- The AOC-WS consists of:
  - Commercial off-the-shelf hardware
  - Software—including Theater Battle Management Core Systems – Force Level and Master Air Attack Plan Toolkit—to enable planning, monitoring, and directing the execution of air, space, and cyber operations
  - Third-party software applications—including Global Command and Control System – Joint (GCCS-J) and Joint Automated Deep Operations Coordination System—to enable joint and interagency integration
  - Additional third-party systems that accept, process, correlate, and fuse command and control data from multiple sources and share them through multiple communications systems
  - Voice, digital, and data communications hardware
- AOC-WS 10.1 operates on several different local area networks (LANs), including the Secret Internet Protocol Router Network, Joint Worldwide Intelligence Communications System, and a coalition LAN, when required. The LANs connect the core operating system and primary applications to joint and coalition partners supporting the applicable areas of operation. Users can access web-based applications through the Defense Information Systems Network.
- The Air Force typically tests major functionality upgrades to AOC-WS 10.1 during a three-phased Recurring Event (RE) test cycle, which includes event-based test periods primarily focused on software upgrades. The three phases of the RE test cycle typically includes:
  - Phase 1: Developmental testing conducted at the CAOC-X located at Joint Base Langley-Eustis, Virginia.
  - Phase 2: Operational testing conducted at CAOC-X to assess effectiveness.
  - Phase 3: Operational testing conducted at a fielded site to assess suitability.
- Testing of lower level, minor functionality upgrades, with assessment of "operational processes," are integrated with the latter portions of developmental testing. For these minor functionality upgrades (as opposed to purely cybersecurity

updates or maintenance-type upgrades), the Air Force uses the term OOC for their testing; i.e. OOC 13.1.
- The future upgrade, AOC-WS 10.2, is designed to deliver a modernized, integrated, and automated approach to AOC operations.
- Command and Control Air Operations Suite-Command and Control Information Services (C2AOS-C2IS) is a software developmental program to upgrade critical AOC-WS mission software, enhancing the ability of operators to perform AOC core tasks more quickly and efficiently, as well as providing new planning and execution capabilities for integrated air and missile defense and net-enabled weapons.

Mission
- The Commander, Air Force Forces or the Joint/Combined Forces Air Component Commander uses the AOC-WS to exercise control of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations to meet operational objectives and guidance.
- The AOC is the senior command and control element of the Air Force's Theater Air Control System and provides operational-level command and control of joint and combined air, space, and cyberspace operations. The AOC's capabilities include command and control of joint theater air and missile defense; preplanned, dynamic, and time-sensitive multi-domain target engagement operations; and intelligence, surveillance, and reconnaissance operations management.

Major Contractors
- AOC-WS 10.1 Production Center: Jacobs Technology Inc., Engineering and Technology Acquisition Support Services – Hampton, Virginia
- AOC-WS 10.2 Modernization: Northrop Grumman – Newport News, Virginia

---

Activity
- In October and November 2015, the Air Force conducted operational testing of AOC-WS 10.1 OOC 13.1 in accordance with the DOT&E-approved test concept briefing and test plans. The primary focus of OOC 13.1 was to upgrade GCCS-J from version 4.2.0.9U2 to version 4.3U1. This upgrade of GCCS-J also required compatibility updates to the Joint Automated Deep Operations Coordination System and Theater Battle Management Core Systems.
- In February 2016, the Air Force conducted operational testing of AOC-WS 10.1 OOC 13.2 in accordance with the DOT&E-approved test concept briefing and test plans. The objectives of OOC 13.2 were to improve the AOC-WS' cybersecurity posture by closing over 200 Category II open deficiencies, upgrading the Master Air Attack Plan Toolkit, adding a Microsoft® active directory users and computer console (ADUC), and upgrading the Airspace Management Application.
- In April 2016, the Air Force completed its reports on OOC 13.1 and OOC 13.2. Both reports included data from integrated testing at CAOC-X.
- In August 2016, the AOC CRB recommended fielding OOC 13.1 and OOC 13.2 because GCCS-J 4.3U1, despite its deficiencies, is a better product than the currently fielded GCCS-J 4.2.0.9U2. The CRB made this decision because DISA failed to deliver a viable update to GCCS-J 4.3U1 that can be integrated into the OOC 13.3 to address OOC 13.1's Category I deficiencies.
- In February and March 2016, AOC-WS 10.2 failed to complete the second of two scheduled phases of developmental testing at CAOC-X. These failures occurred after contractor remediation actions taken as a result of Cure Notices issued in September 2014 and September 2015. A Cure Notice is a letter from the government to the contractor regarding concerns about poor performance in accordance with contract requirements. The severity and quantity of the functional and cybersecurity deficiencies identified during the first half of developmental testing resulted in the cancelation of the remaining developmental test events and planned operational assessment activities. Currently, the program is conducting a Critical Change Review.
- In June and July 2016, the Air Force conducted early developmental testing on several C2AOS-C2IS capability packages. These and subsequent developmental test events are precursors to integrating all the capability packages into a single software release that will be integrated into the AOC-WS baseline and then undergo IOT&E.

Assessment
- The Air Force adequately tested AOC-WS 10.1 OOC 13.1 and OOC 13.2 with an assessment of operational processes during integrated developmental/operational test events.
- OOC 13.1 was found to be not operationally effective due to three open Category I deficiencies against third-party software that affect AOC operations in two critical ways:
  - No acceptable public key infrastructure-enabled user authentication capability, which is required for access to GCCS-J integrated imagery and intelligence applications.
  - Due to the excessive track clutter that results in an unusable common operational picture (COP) display, operators are unable to monitor and assess electronic warfare threats. In addition, there is insufficient source information to enable COP managers to resolve these track clutter problems.
- Initially, OOC 13.1 was found to be operationally suitable with limitations. The upgrade could not be conducted without extensive Tier 2 Help Desk direct onsite interaction with the build team. However, subsequent software supplements and

improved build documentation resolved the issues, improving the assessment to operationally suitable.

- A cybersecurity evaluation of OOC 13.1 resulted in no significant findings and concluded that the results from RE13 (completed in August 2015) remain valid. However, the OOC 13.3 test concept includes a full Cooperative Vulnerability and Penetration Assessment of the OOC 13.1 functional capabilities along with the OOC 13.3 upgrades and fixes, and should provide an updated assessment of the baseline cybersecurity posture.
- OOC 13.2 was found to be operationally effective and suitable. During testing, four Category II cybersecurity deficiencies associated with ADUC increased the risk to the AOC-WS baseline. Consequently, the Air Force removed ADUC from OOC 13.2 until the deficiencies can be resolved, targeting ADUC for incorporation into RE15. Additionally, since OOC 13.2 cannot be implemented without the successful installation of OOC 13.1, its fielding was delayed while the Air Force attempted to resolve the OOC 13.1 issues.
- Air Combat Command initially decided not to field OOC 13.1 until the Category I deficiencies are fixed. Resolution of the Category I deficiencies was scheduled to be accomplished in OOC 13.3 in November and December 2016; however, DISA failed to provide the Program Management Office with viable updates. Therefore, despite the Category I deficiencies, the AOC CRB recommended fielding OOC 13.1, along with OOC 13.2, beginning in September 2016. These would enable delivery of upgraded capabilities to meet other warfighter operational requirements. Resolution of OOC 13.1 deficiencies are planned to be delivered as part of RE15, scheduled to be tested in April and May 2018.
- The key to successful testing and fielding of AOC-WS 10.1 continues to be close collaboration between the AOC-WS Program Office and the providers of third-party applications to ensure those applications meet the operational and cybersecurity needs of the AOC. Early AOC-WS tester involvement in third-party testing continues to be necessary to identify critical problems for early corrective action.

Recommendations

- Status of Previous Recommendations. The Air Force has made progress on one FY15 recommendation by developing and testing software updates that close cybersecurity vulnerabilities. However, the more secure software has not yet been deployed because of operational deficiencies, and new deficiencies have been identified with third-party software. The Air Force still needs to address the FY15 recommendations to improve dynamic cyber defensive capabilities focused on detecting and responding to cyber-attacks against the AOC-WS, and to reassess the Help Desk-enabling concept to support the build process. Additionally, the Air Force still plans to address a long-standing requirement to collect and report reliability, availability, and maintainability (RAM) data to the Program Office and DOT&E by implementing a technical RAM collection solution in the modernization increment, AOC-WS 10.2.
- FY16 Recommendations. None.

B-2 Defensive Management System Modernization (DMS-M)

Executive Summary

- In FY16, the Air Force developed a revised acquisition and test strategy for the B-2 Defensive Management System Modernization (B-2 DMS-M) program in support of an acquisition Milestone B decision. DOT&E approved the B-2 DMS-M Milestone B Test and Evaluation Master Plan (TEMP) in October 2015. USD(AT&L) approved program entry into the engineering, manufacturing, and development (EMD) phase on March 24, 2016.
- Contractor design activities are in progress, leading to a system-level critical design review in early FY17. Planning is in progress to modify a single B-2 test aircraft with new system components in FY17 to support installed system testing in the Benefield Anechoic Facility (BAF) at Edwards AFB, California. Developmental flight tests will begin in FY18, leading to an Air Force Operational Test and Evaluation Center (AFOTEC) operational assessment in FY19 and IOT&E in FY20.
- Beginning in FY17, the DOD Electronic Warfare Infrastructure Improvement Program (EWIIP) will deliver improved test range capabilities that are highly relevant to B-2 DMS-M operational testing. It is essential that the B-2 DMS-M program incorporate these improved threat representations, as they become available, into planned developmental and operational flight test events.
- The development of AFOTEC modeling and simulation (M&S) validation plans for the B-2 Weapons Support and Sustainment Center (WSSC) facility and related M&S tools is a critical early test planning requirement. Clear definition and approval of operational test M&S validation data requirements – in advance of planned FY18 BAF risk-reduction testing – is required to ensure efficient use of this early test opportunity.

System

- The B-2 is a two-pilot, long-range, air-refuelable, all-weather bomber aircraft designed to employ both nuclear and non-nuclear precision-guided weapons. It incorporates stealth technologies to reduce radar cross section and minimize electronic, infrared, acoustic, and visual signatures.
- B-2 mission systems include a GPS-aided precision navigation system, strategic radar targeting system, electronic support measures, and worldwide communications and data transfer systems.
- The B-2 can carry up to 50,000 pounds of munitions in internal bomb bays. Current weapons capabilities include a wide range of both nuclear and non-nuclear precision-guided munitions.

- The B-2 DMS-M upgrades include a digital electronic support measures (ESM) subsystem, new ESM antennas, and modern display processing units to improve threat radar detection, identification, and avoidance capabilities. Associated software components integrate these upgraded systems with existing B-2 avionics systems to improve overall pilot threat awareness, threat reaction, and survivability.

Mission

- Theater Commanders primarily use B-2 bomber aircraft to accomplish worldwide nuclear and conventional missions intended to find, fix, target, engage, and assess heavily defended, high-value targets located in denied adversary airspace.
- B-2 theater mission tasks include strategic attack, time-sensitive targeting, air interdiction, suppression/destruction of enemy air defenses, and nuclear deterrence.

Major Contractor

Northrop Grumman Aerospace Systems – Redondo Beach, California

Activity

- In FY16, the Air Force developed a revised acquisition and test strategy for the B-2 DMS-M program in support of an acquisition Milestone B decision. DOT&E approved the B-2 DMS-M Milestone B TEMP in October 2015. USD(AT&L) approved program entry into the EMD phase on March 24, 2016. The approved program schedule includes a Milestone C Low-Rate Initial Production decision in FY19, followed by IOT&E and the Full-Rate Production decision in FY20.
- Contractor design activities are in progress, leading to a system-level critical design review in early FY17. Following design approval, the program plans to conduct extensive hardware-in-the-loop laboratory and digital simulation risk reduction testing. Planning is in progress to modify a single B-2 test aircraft with new system components in FY17 to support installed system testing in the BAF at Edwards AFB, California. Developmental flight tests will begin in FY18, leading to an AFOTEC operational assessment in FY19 and IOT&E in FY20.
- The approved Air Force operational test strategy includes evaluation of B-2 defensive system performance in the open-air test range environment, leveraging new adversary threat system emulation capabilities provided by the EWIIP. The AFOTEC strategy also includes an extensive digital M&S component to evaluate performance in more advanced threat environments. AFOTEC is currently developing validation and verification plans necessary to support accreditation of the B-2 WSSC laboratory and other tools for operational test purposes.

Assessment

- The approved B-2 DMS-M TEMP defines a highly integrated developmental and operational test strategy that includes open-air test range missions as the most critical component. Beginning in FY17, EWIIP will deliver improved test range capabilities that are highly relevant to B-2 DMS-M operational testing. It is essential that the B-2 DMS-M program incorporate these improved threat representations, as they become available, into planned developmental and operational flight test events to support an adequate evaluation of operational effectiveness and suitability.
- Development of AFOTEC M&S validation plans for the B-2 WSSC facility and related M&S tools is a critical early test planning requirement. Clear definition and approval of operational test M&S validation data requirements, in advance of planned FY18 BAF risk-reduction testing, is required to ensure efficient use of this early test opportunity.
- Due to operational priorities and the small B-2 fleet size, the B-2 DMS-M program must rely on a single test aircraft to support the entire 3-year developmental and operational ground and flight test program. Reliance on a single test asset significantly increases schedule execution risk. Limited test asset availability will also require close coordination between developmental and operational test organizations to meet program test requirements and schedule milestones.
- Previous B-2 operational test periods have incorporated only limited cybersecurity vulnerability and adversarial assessments. The B-2 DMS-M TEMP defines a more extensive cybersecurity test strategy comprised of progressive test events leading to a full IOT&E assessment of system-level cybersecurity status. Detailed planning and execution of this strategy is a critical IOT&E requirement.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The B-2 Program Office and AFOTEC should:
  1. Coordinate B-2 DMS-M M&S validation and verification plans with DOT&E in advance of the planned installed system testing in BAF scheduled for FY17. These plans should also include validation data requirements to be collecting during integrated flight test events planned to begin in FY18.
  2. Coordinate with DOT&E to incorporate more advanced threat scenarios, based on new EWIIP threat emulation capabilities, into integrated test events and operational flight test plans.

Battle Control System – Fixed (BCS-F)

Executive Summary

- The Air Force completed a Force Development Evaluation (FDE) to evaluate operational effectiveness; interoperability; operational suitability; impact on tactics, techniques, and procedures; and cybersecurity postures on the Battle Control System – Fixed (BCS-F) Increment 3, Release 3.2.3 (R3.2.3) at all U.S. air defense sites in April 2016.
- BCS-F R3.2.3 is still not survivable against potential cyber-attacks despite the Air Force's efforts to resolve critical cybersecurity deficiencies.
- The BCS-F R3.2.3 has operational effectiveness deficiencies in system track management and datalink operations. The operators are able to use workarounds to mitigate these deficiencies to an acceptable level.
- The BCS-F R3.2.3 is operationally suitable with deficiencies in:
  - System maintenance documentation
  - Training program on system operations and maintenance
  - Lack of cybersecurity policies
  - Lack of program life cycle management policies and plan (i.e. Help Desk management, maintenance and repairs reporting, and spares management)
- All U.S. air defense sites were utilizing R3.2.3 in April 2016. Upon completion of the FDE, the Air Force formally fielded R3.2.3.

System

- BCS-F is the tactical air surveillance and battle management command and control system for the continental U.S. and Canadian air defense sectors (ADS)—Eastern ADS, Western ADS, Canadian ADS—of the North American Aerospace Defense Command (NORAD), the NORAD Alaska Regional Air Operations Center (RAOC), and U.S. Pacific Command's (PACOM) Hawaii RAOC.
- The system utilizes commercial off-the-shelf hardware within an open-architecture software configuration and operates within the NORAD and PACOM air defense architecture.
- The BCS-F R3.2.3 software upgrade includes the following system enhancements:
  - Increases maximum sensor and radar processing capacity, from 200 to 300 sensors
  - Fixes for 12 cybersecurity deficiencies previously identified
  - Updates to the air defense sector site radar parameters
  - Fixes for the operations display and the graphical user interface
  - Upgrades to the Internet Protocol converter/radar interface
- Also, the BCS-F R3.2.3 upgrade provided the following changes to system sustainment:
  - A software development/logistics support transition from contractor to government (520 Software Maintenance Squadron)
  - Updated Technical Order and System Manual documentation
  - Updated system training materials
- BCS-F R3.2.3 was designed to include the capability to interface with and process data from a sensor in the Wide Area Surveillance (WAS) program.
  - Due to WAS' lack of readiness, the Air Force did not conduct operational testing of WAS with BCS-F R3.2.3, but will evaluate sensor integration during operational testing of BCS-F R3.2.4.

Mission

- The Commander, NORAD and Commander, PACOM use BCS-F to execute command and control and air battle management to support air sovereignty and air defense missions for North American Homeland Defense and PACOM air defense.
- Air defense operators employ BCS-F to conduct surveillance, identification, and control of U.S. sovereign airspace and control air defense assets, including fighters, to intercept and identify potential air threats to U.S. airspace.

Major Contractor

Raytheon Systems – Fullerton, California

Activity

- From November 2015 through April 2016, the 605th Test and Evaluation Squadron conducted FDE on BCS-F R3.2.3 at all U.S. ADSs in accordance with a DOT&E-approved Test and Evaluation Master Plan and test plan.

- Upon completion of the FDE, the Air Force formally fielded R3.2.3. All U.S. ADSs were utilizing BCS-F R3.2.3 by April 2016.
- Canadian Air Defense Forces operationally accepted R3.2.3 in June 2016.

Assessment

- BCS-F R3.2.3 resolved 22 deficiencies in operational effectiveness and suitability associated with battle management and support operations.
  - These deficiencies were discovered during previous Increment 3.2 (R3.2, R3.2.0.1, R3.2.2) operational testing events.
  - Developmental testing and FDE of BCS-F R3.2.3 revealed 45 new deficiencies associated with battle management and support operations.
  - Operational testing of BCS-F R3.2.3 revealed two significant effectiveness deficiencies in system track management and two significant deficiencies in datalink operations.
  - Operator workarounds mitigated these deficiencies to an acceptable level.
- Although the Air Force did not collect sufficient operational test data to demonstrate the availability and reliability requirements with statistical confidence, BCS-F R3.2.3 is assessed as maintainable and reliable.
  - During 1,134.68 hours of testing, BCS-F R3.2.3 experienced 7 minutes of downtime in order to troubleshoot two system failures (a Category I and a Category II) at NORAD's Eastern ADS. This resulted in an operational availability of 99.99 percent (the 80 percent confidence interval is 99.79 to 99.99 percent).
  - Due to a lack of effective life-cycle management policies and plan, accurate data to assess overall system availability and reliability were not available.
  - BCS-F R3.2.3 was maintainable for routine maintenance actions, but the observed Mean Time Between Corrective Maintenance Action (MTBCMA) of 17 hours did not meet the requirement of 100 hours. This was not a critical shortfall since the maintenance actions had no negative effect on operations or operator workload.
  - After further analysis of maintenance activity, two types of maintenance actions were identified: Critical Field Repair and Non-Critical Field Repair.
  - A Critical Field Repair is assessed when a fault, failure, or malfunction results in the loss of any system's mission essential function as specified in the mission essential system list. Also, a critical failure includes greater than 10 percent of operator workstations becoming inoperative. A failure is not considered critical if mission operations are restored within 2 minutes.
  - MTBCMA for Critical Field Repair Actions (2 failures) was 211 hours and MTBCMA for Non-Critical Field Repair Actions (76 failures) was 17 hours.
  - In order to better understand system maintainability, future assessments may require separating Critical and Non-Critical MTBCMA measurements and identifying appropriate threshold requirements for each.
- While BCS-F R3.2.3 is operationally suitable, technical documentation and training for the system remains deficient. These deficiencies include:
  - System maintenance documentation
  - Training program on system operations and maintenance
  - Lack of cybersecurity policies
  - Lack of program life-cycle management policies and plan (i.e. Help Desk management, maintenance and repairs reporting, and spares management)
- Since only minor cybersecurity fixes were included in BCS-F R3.2.3, DOT&E assesses R3.2.3 remains deficient in all cybersecurity assessment areas. The system is poorly equipped to protect, detect, react, and restore/recover from attacks by current cyber threats, despite the fact that BCS-F R3.2.2 was designed to resolve many critical cybersecurity deficiencies. To address previously identified deficiencies, the Air Force implemented the Computer Network Defense Service Provider (CNDSP) agreement in 1QFY15. However, the Air Force has not conducted a cybersecurity assessment of BCS-F since the CNDSP was implemented.

Recommendations

- Status of Previous Recommendations. The Air Force satisfactorily addressed three of the previous recommendations. The Air Force still needs to:
  1. Correct and formalize all BCS-F Increment 3 system documentation and training deficiencies.
  2. Develop a plan for remote workstation management to include sustainment, training, documentation, and cybersecurity compliance.
  3. Upgrade the System Support Facility to support a more robust BCS-F developmental and operational testing capability in order to minimize the impact of overall testing at the operational air defense sector sites.
  4. Improve reliability to meet the threshold requirement for MTBCMA.
  5. Re-assess system cybersecurity vulnerabilities and correct identified cybersecurity deficiencies.
  6. Re-evaluate BCS-F survivability against cyber-attacks after the CNDSP has been implemented.
  7. Ensure appropriate policies, procedures, and tools exist for system administrators to effectively detect unauthorized intrusions.
- FY16 Recommendations. The Air Force should:
  1. Correct system operational effectiveness deficiencies.
  2. Correct and formalize all BCS-F R3.2.3 system operations and maintenance documentation, policy, and training deficiencies.
  3. Update the system threat assessment report for BCS-F.

CV-22 Osprey

Executive Summary

- Air Force Special Operations Command (AFSOC) conducted CV-22 testing to evaluate Tactical Software Suite (TSS) 20.2.02/20.2.03, which is a compilation of software and hardware packages.
- The Mission Computer Obsolescence Initiative (MCOI) upgrade portion of TSS allowed pilots to use MCOI-compatible planning tools to create and load mission plans into the aircraft systems.
- Both pilots and maintainers commented that the training provided for MCOI was not sufficient and more was required.
- The Color Helmet-Mounted Display (CHMD) system degraded pilot situational awareness during both day and night flights and was not reliable.
- The Generation 5 radios did not provide an improvement to CV-22 communications capabilities and did not resolve workload problems.

System

- The CV-22 is the AFSOC variant of the V-22. It replaced Special Operations Forces MH-53 helicopters in 2008. The tilt-rotor design provides the speed and range of a conventional fixed-wing aircraft and vertical take-off and landing capabilities of a helicopter.
- The CV-22 has terrain-following/terrain-avoidance radar, an advanced multi-frequency radio communication suite, an integrated electronic defense suite, and aerial refueling capability, allowing it to augment the AFSOC MC-130 fleet.
- The CV-22 electronic defensive suite includes the Suite of Integrated Radio Frequency Countermeasures (SIRFC) and the Directional Infrared Countermeasures (DIRCM) system with the AAR-54 Missile Warning Sensor, Small Laser Transmitter Assembly jammer, and the ALE-47 Countermeasure System capable of dispensing both flares and chaff. The Dedicated Electronic Warfare Display provides an integrated threat picture to the crews from SIRFC and DIRCM.
- The CV-22 can carry 18 combat-ready Special Operators 538 nautical miles and return. It can self-deploy up to 2,100 nautical miles with one aerial refueling.
- The Advanced Ballistic Stopping System (ABSS) is an optional protective armor kit that CV-22 squadrons can install for certain mission scenarios. The ABSS kit weighs 825 pounds.
- Bell-Boeing has delivered 51 of 52 purchased aircraft which includes one combat loss and one training loss. The final aircraft is expected to be delivered by the end of 2016.

Mission

Commanders employ AFSOC squadrons equipped with the CV-22 to provide high speed, long-range insertion and extraction of Special Operations Forces to and from high-threat objectives.

Major Contractors

- Bell-Boeing Joint Venture:
  - Bell Helicopter – Amarillo, Texas
  - The Boeing Company – Ridley Township, Pennsylvania
- The Protective Group, Inc. – Miami Lakes, Florida

Activity

- AFSOC's Operational Test Squadron, the 18th Flight Test Squadron (FLTS), conducted operational testing on the CV-22 TSS 20.2.02/20.2.03, which is a compilation of software and hardware upgrades, between October 1, 2015, and February 19, 2016. The 18th FLTS conducted the testing in accordance with the DOT&E-approved test plan.
- The 18th FLTS evaluated the updated TSS, which includes MCOI upgrades, JVX [Joint Services Advanced Vertical Lift Aircraft] Application System Software (JASS), a CHMD system, a Generation 5 AN/ARC 210 radio, and MCOI-compatible mission planning tools. The MCOI brings increased processor speed and capacity, will be included as the standard mission computer in all new-build V-22 aircraft, and will eventually be retrofitted into all V-22s. This testing updated the findings on the TSS 20.2.01 deficiencies reported in FY15.
- The Joint Live Fire test program completed supplemental testing of the ABSS armor in July 2016. The testing evaluated one additional threat type, additional obliquity angles, edge performance, and installed armor performance. This

additional testing was in response to gaps identified with the initial testing performed in 2014.
- AFSOC completed a portion of the upgraded SIRFC software version 8 tests in February through March 2015 at China Lake and the Nevada Test and Training Range to address CV-22 SIRFC active countermeasure deficiencies. AFSOC completed the remaining testing of the SIRFC software in October 2015.
- The Air Force's 46th Test Squadron in cooperation with the 18th FLTS conducted a Cooperative Vulnerability and Penetration Assessment of CV-22 cybersecurity protections and vulnerabilities in September 2016. This testing included the first investigations of Military Standard 1553 data bus cybersecurity on any V-22 aircraft. The data and results from this testing will be available in FY17.

Assessment
- The CHMD Color Display Day Module degraded CV-22 pilots' situational awareness and was not reliable during testing.
- The CHMD Color Display Night Module degraded CV-22 pilots' situational awareness while they were operating in brightly illuminated areas such as populated shorelines and urban areas.
- Pilots commented that they did not receive sufficient training on CHMD use and that they needed more training flights using the CHMD.
- CV-22 pilots were able to use the MCOI-compatible mission planning tools to create mission plans and load them onto the CV-22 aircraft systems. Pilots reported that the requirement to manually load hazard data was time-consuming, cumbersome, and increased mission-planning time by up to an hour.
- CV-22 maintenance personnel commented that they were not provided sufficient training to troubleshoot or repair the new MCOI mission computer.
- The Generation 5 radios did not provide an improvement to CV-22 communications capabilities and did not resolve workload problems identified in IOT&E.
- During TSS testing, operational test pilots reported frequent faults in the Icing Protection System (IPS).
  - AFSOC examined their fleet-wide data on the IPS, which revealed a mean time between failure of 37 hours for the period of March 2015 to February 2016. Availability of the fully-capable IPS systems across AFSOC was 43 percent with the highest availability among those units who have the highest potential for flight in icing conditions.
  - IPS failures affect other aircraft components. For example, 15 percent of failures charged to proprotor blades were caused by failure of IPS components on the blade. Poor IPS reliability increases sustainability costs and affects CV-22 employment in known or suspected icing. It can cause safety-of-flight issues if inadvertent icing is encountered.
  - Low availability/reliability of the IPS is a change from performance observed in 2013 IPS tests and could affect CV-22 suitability.
- Preliminary findings indicate the ABSS armor demonstrated better coupon performance than the 2014 testing. Aircraft shielding enhances the armor's performance and mitigates previously identified problems.
- Preliminary data analyses suggest that the active countermeasure component of the SIRFC 8.02 system did not address the subsystem deficiencies. Consistent with previous results, the subsystem does not meet most survivability requirements.
- AFSOC will publish the cybersecurity test results and analysis in FY17.

Recommendations
- Status of FY15 Recommendations. The Navy completed operational testing of SIRFC and conducted the recommended live fire testing.
- FY16 Recommendations. The Navy and AFSOC should:
  1. Investigate the causes of poor performance and reliability failures of the CHMD, reduce the time required to load mission data, improve maintenance training for MCOI maintainers, and continue efforts to improve air-to-ground communications.
  2. Investigate IPS reliability and determine if additional design changes are needed to increase IPS availability and reduce CV-22 supportability costs.

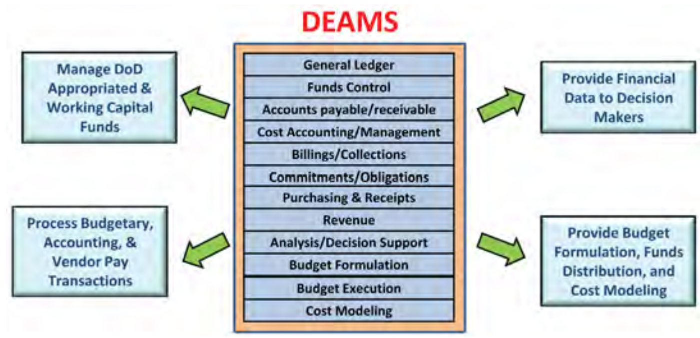
Defense Enterprise Accounting and Management System (DEAMS)

Executive Summary

- In accordance with a September 30, 2015, Acquisition Decision Memorandum, the Air Force Operational Test and Evaluation Center (AFOTEC) conducted a Verification of Fixes (VoF) test on the Defense Enterprise Accounting and Management System (DEAMS). AFOTEC planned to conduct the VoF test at four bases with the participation of three Air Force Major Commands, three U.S. Combatant Commands, and the Defense Finance and Accounting Service (DFAS), from January 4 – 29, 2016. However, the Program Executive Officer (PEO) stopped the VoF test after two bases (Scott AFB and Keesler AFB), when the data indicated that multiple Key Performance Parameters (KPPs) could not be met.
- The VoF test demonstrated that DEAMS remains not operationally effective and not operationally suitable. In the area of effectiveness, DEAMS Increment 1 did not effectively perform several critical accounting and management tasks, four of which were KPPs. DEAMS suitability issues included configuration management and usability as users continue to avoid using DEAMS to conduct financial analysis and reporting.
- DEAMS remains not survivable in the expected cybersecurity threat environment. Following IOT&E, the Program Management Office (PMO) conducted limited cybersecurity testing. From November 18 – 19, 2015, a cybersecurity test team conducted an event to assess three cybersecurity fixes. The team conducted this test on the live network in the pre-production environment, and verified that only one of the three fixes was successful. Subsequent cybersecurity testing demonstrated that another cybersecurity fix was successful on a single server in the DEAMS enclave. However, the cybersecurity deficiency still existed on two other servers in the enclave, indicating that the PMO's processes and procedures to prevent recurrence of cybersecurity problems are not yet adequate.

System

- DEAMS Increment 1 is a Major Automated Information System that uses commercial off-the-shelf Enterprise Resource Planning software to provide accounting and management services.
- The DEAMS Increment 1 PMO is following an evolutionary acquisition strategy that adds additional capabilities and users incrementally. There are six scheduled releases. The Air Force anticipates over 15,000 users worldwide will use DEAMS by the end of the increment.
- DEAMS Increment 1 is intended to improve financial accountability by providing a single, standard, automated financial management system that is compliant with the Chief Financial Officers Act of 1990 and other mandates. DEAMS Increment 1 performs the following core accounting functions:
  - Core Financial System Management
  - General Ledger Management
  - Funds Management
  - Payment Management
  - Receivable Management
  - Cost Management
  - Reporting
- DEAMS interfaces with approximately 40 other systems that provide travel, payroll, disbursing, transportation, logistics, acquisition, and accounting support.
- DEAMS supports financial management requirements in the Federal Financial Management Improvement Act of 1996 and DOD Business Enterprise Architecture. Therefore, DEAMS is a key tool for helping the DOD to have its financial statements validated as ready for audit by the end of FY17 as required by the National Defense Authorization Act for FY10.



Mission

Air Force financial managers and tenant organizations use DEAMS Increment 1 to do the following across the Air Force, U.S. Transportation Command, and other U.S. component commands:

- Compile and share accurate, up-to-the-minute financial management data and information
- Satisfy Congressional and DOD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework

Major Contractor

Accenture Federal Services – Dayton, Ohio

Activity

- In accordance with a September 30, 2015, Acquisition Decision Memorandum, AFOTEC conducted a VoF test on DEAMS. AFOTEC planned to conduct the VoF test at four bases with the participation of three Air Force Major Commands, three U.S. Combatant Commands, and DFAS, from January 4 – 29, 2016. However, the PEO stopped the VoF test after two bases (Scott AFB and Keesler AFB), when the data indicated that multiple KPPs could not be met. Therefore, AFOTEC completed testing at only two of the four test locations.
- In preparation for the VoF test, the Army Research Laboratory at White Sands Missile Range, New Mexico, supported the PMO in conducting a limited cybersecurity Cooperative Vulnerability and Penetration Assessment at Maxwell AFB – Gunter Annex, Alabama.
- The Joint Interoperability Test Command (JITC) completed a DEAMS Increment 1 interoperability evaluation in August 2016.
- AFOTEC conducted the VoF test in accordance with the DOT&E-approved Test and Evaluation Master Plan and the test plan.

Assessment

- DEAMS Increment 1 remains not operationally effective and not operationally suitable. DEAMS Increment 1 did not effectively perform several critical accounting and management tasks, four of which were KPPs. Some key effectiveness findings from the IOT&E and VoF test are as follows:
  - DEAMS does not provide an accurate balance of available funds to meet the KPP requirement. During the VoF test, only 62 percent (33 out of 53) of the balance queries were accurate, versus a 98 percent requirement.
  - DEAMS continues to have problems with interoperability with other systems, which contribute to the poor accuracy results discussed above. According to the August 2016 JITC interoperability report, four critical interfaces did not meet criteria due to timeliness problems which have a moderate to major impact on interoperability with two critical interfaces: the Centralized Disbursing System and Departmental Cash Management System.
  - Users continue to rely on the Commanders' Resource Integration System and other legacy systems for reporting instead of using the DEAMS Discoverer tool. Oracle Business Intelligence Enterprise Edition (OBIEE), the DEAMS replacement for Discoverer, has provided improved reporting capabilities on other programs (e.g., Defense Agencies Initiative), but challenges remain for implementation of OBIEE.
  - Transaction backlog continues to be a major problem with DEAMS. Transaction backlogs decreased during the summer of 2015, but increased in the fall and remained substantially above the low point seen during the previous months. At the start of the VoF test, the transaction backlog was near 20,000 transactions.
  - In both the IOT&E and VoF, the transaction backlog was a major contributor to the inadequate performance of DEAMS. The transaction backlog causes a transaction to take longer than normal to post on the General Ledger, which in turn causes inaccuracies in DEAMS reports, to include the Status of Funds.
  - Depending upon the type of backlogged transaction, an un-posted transaction can result in interest penalty payments on aged transactions, affecting timely decision-making and requiring additional manpower for DFAS staff to process backlog transactions.
- Numerous high-severity incident reports, deficiencies, and system change requests (SCRs) remain. The numbers of Severity 2 and 3 defects and SCRs are noted in Table 1 (Severity 2 problems adversely affect DEAMS and do not have a sustainable work around, while Severity 3 problems adversely affect DEAMS but have a sustainable work around). Of the 114 unresolved defects reported by the DEAMS Functional Management Office as of July 2016, 55 (48 percent) were over 8 months old. Of the 318 SCRs reported as of July 2016, 217 (68 percent) were over 8 months old.

Table 1: Defects and SCRs from prior to and after VoF

	November 2015	July 2016
Severity 2 Defects	52	34
Severity 3 Defects	174	68
Severity 2 System Change Requests (SCRs)	52	96
Severity 3 SCRs	204	186

- The DEAMS PMO is not following its own configuration management procedures, which prescribe rigorous developmental and regression testing prior to fielding new software releases. The PMO sharply reduced developmental and regression testing starting in August 2014 to meet a fixed deployment schedule. This led to the fielding of defective software; this software is likely a major contributor to the backlog problems that continue to affect DEAMS users. DEAMS regression testing has recently increased to cover close to 60 percent of the business processes. The PMO should implement regression scripts to test all critical interfaces in DEAMS.
- Where it is possible to do so, users continue to avoid using DEAMS to conduct financial analysis and reporting. For example, Keesler AFB users export DEAMS data to spreadsheets to perform analyses and reporting rather than use corresponding DEAMS functionality. Additionally, PMO data from the months of September and October 2015 indicate that users generated Status of Funds reports less than once per week on average per user. These reports are critical to end-of-month and fiscal year-end closeouts; therefore, these data indicate that most of the approximately 11,000 DEAMS

users are using legacy systems instead of DEAMS to evaluate fund status.

- DEAMS remains not survivable in the expected cybersecurity threat environment. Following IOT&E, the PMO conducted limited cybersecurity testing. From November 18 – 19, 2015, a cybersecurity test team conducted a limited event to assess three cybersecurity fixes. The team conducted this test on the live network in the pre-production environment, and verified that only one of the three fixes was successful. Subsequent cybersecurity testing demonstrated that another cybersecurity fix was successful on a single server in the DEAMS enclave. However, the cybersecurity deficiency still existed on two other servers in the enclave. This indicates that the PMO's processes and procedures to prevent recurrence of cybersecurity problems are not yet adequate. However, the PMO instituted improved cybersecurity processes by adding the cybersecurity problems to the deficiency management system for visibility and action, instituted dedicated cybersecurity patch releases, and reprioritized all cybersecurity findings for correction or risk acceptance.

Recommendations

- Status of Previous Recommendations. The Program Office did not satisfy the FY15 recommendations to:
  1. Correct balance accuracy defects in accordance with KPP requirements and demonstrate progress towards DEAMS Increment 1 achieving full auditability.
  2. Identify and implement processes, procedures, and software improvements to clear the transaction backlog to fix the lag time between transaction and posting of transaction, and to ensure accurate and timely reporting.
  3. Conduct regression testing to improve DEAMS Increment 1 performance and identify potential interface problems before fielding software updates and releases.
  4. Provide DEAMS Increment 1 training that prepares users to effectively employ DEAMS Increment 1 upon fielding.
  5. Work with AFOTEC to conduct follow-on operational testing to verify that the deficiencies have been corrected and that the new reporting tool is operationally effective, suitable, and survivable, once corrections have been made and a new reporting tool has been fielded.
- FY16 Recommendations. The DEAMS Program Manager should:
  1. Cease allowing DEAMS to be schedule-driven and delay DEAMS deployments, until the PMO fixes the backlog of high-severity deficiencies and shows that the system works properly during operationally realistic testing.
  2. Determine the root causes of the transaction backlogs and other anomalies that have appeared since the fielding of deficient software in August 2014 and make a concerted effort to clear remaining backlogs.
  3. Conduct FOT&E with a pilot set of users, prior to further deployments, to confirm DEAMS is operationally effective, operationally suitable, and survivable.
  4. Complete integration and testing of the OBIEE reporting tool and demonstrate effectiveness through operational testing to allow the retirement of Discoverer and fielding of OBIEE.
  5. Develop necessary regression testing scripts to ensure that all critical DEAMS interfaces are adequately tested.
  6. Complete mitigation of all cybersecurity vulnerabilities.

E-3 Airborne Warning and Control System (AWACS) Block 40/45

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) completed the IOT&E for the E-3 Airborne Warning and Control System (AWACS) Block 40/45 Modification during 2010. DOT&E and AFOTEC evaluated the system as operationally effective but not operationally suitable. Key deficiency areas included reliability and training. In addition, the Block 40/45 ground-based and deployable support systems were not available and operational testing of these elements was deferred to the FOT&E.
- The E-3 Block 40/45, designated E-3G, modifications include incremental updates to the business-grade commercial mission computing systems in the aircraft, ground support systems, and application software to address diminishing manufacturing resources, correction to deficiencies identified through testing and operational use, and to add enhancements. AFOTEC used E-3G hardware version l.0 for IOT&E and version 3.0 for some FOT&E events. The Air Force has fielded both versions.
- The Air Force conducted the following test events:
  - E-3G FOT&E began during 4QFY15, in accordance with the DOT&E-approved Test and Evaluation Master Plan, with the collection of suitability data on the version 3.0-configured E-3G aircraft.
  - Cold weather operational testing during 2QFY16.
  - A cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) and a comparative operational assessment of maritime surveillance and tracking in 3QFY16.
  - An operational deployment and observation of the deployed performance and suitability of the E-3 Block 40/45 and Deployable Ground System during a Red Flag Large Force Exercise in 4QFY16.
- Observations and emerging results from these events indicate that Block 40/45 version 3.0 with mission computing software version 11.1 has deficiencies related to multi-source track integration, maritime tracking, cybersecurity vulnerabilities, and software reliability.
- The Air Force halted completion of FOT&E during the Operational Test Readiness Review largely due to adverse pretest predictions provided by AFOTEC. Instead, AFOTEC was requested to observe employment during a Red Flag Exercise and provide feedback on required improvements to prepare for FOT&E.

System

- E-3 AWACS is built on a Boeing 707 airframe. The AWACS crew employ a surveillance radar and Identification Friend or Foe (IFF) system located in the rotodome above the airframe. Additionally, the E-3 AWACS' communications suite includes ultra high frequency, very high frequency, high frequency radios, satellite communications; and Link 16 and Link 11 tactical datalinks. The E-3 AWACS Block 30/35 upgrade included an Electronic Support Measures (ESM) system – passive detection of electronic signals – mounted on the cheeks of the airframe, under the nose, and in the tail.
- The Block 40/45 upgrade, designated the E-3G, replaces the mission computing system with open-architecture, commercial off-the-shelf hardware including servers and 15 mission crew interactive operator workstations. Also, the Block 30/35 Air Operations Computer Program has been replaced by the Block 40/45 mission computing software program; a set of local area networked, open architecture programs. The human-computer interface is built on the Windows operating system and licenses the Raytheon Solipsys Tactical Display Framework.
- The E-3G's mission computing system provides the capability to automatically fuse all on- and off-board sensor inputs to provide a single track for each air, sea, and land entity using a multi-sensor integration algorithm. The upgrade is also intended to provide:
  - An update to the E-3 AWACS Link 16 and satellite communications capabilities
  - Software to automatically refresh the onboard database
  - An updated mission system health monitoring tool
  - Improved interfaces and controls of the onboard ESM system
  - Improved mission planning and post-mission processing capabilities
- Also, the E-3G upgrade will include a deployable ground support system to enable deployed crews to conduct mission planning and post mission processing with a central data processing center for data storage and retrieval.

- The first six Block 40/45 E-3s are planned to have three different mission computing configurations. The Air Force plans to use the configuration of the seventh Block 40/45 E-3 to upgrade the next 11 jets.
- The AWACS Block 40/45 requires several new ground support systems, including the mission planning system, which the contractor delivered with the first upgraded aircraft. The contractor delivered a deployable mission planning system in support of Initial Operational Capability and trainers for maintenance personnel and mission crew.
- The Air Force is developing new communications and combat identification capability upgrades for the E-3 AWACS that will require integration with E-3G's mission computing system, the human-computer interface software, or both. These upgrades will improve and enhance data communications capabilities; tactical datalink management; and surveillance and identification operations.

Mission

Joint/Combined Forces Air Component Commanders use AWACS-equipped units to:

- Provide airborne early warning, airborne air surveillance and identification, air operations battle management, and beyond line-of-sight capabilities.
- Provide command and control of offensive and defensive counter-air and counter-sea operations, and strike missions including dynamic targeting, close-air support, suppression of enemy air defenses, and strategic attack.
- Manage air refueling operations, combat search and rescue missions, and special operations missions.

Major Contractor

Boeing Corporation – Seattle, Washington

Activity

- The Air Force did not conduct any developmental testing for Block 40/45 hardware configuration version 3.0. There are no dedicated test E-3 aircraft or government laboratories. DOT&E and AFOTEC leveraged operational and training flights from the 552nd Air Control Wing to collect data and were provided dedicated aircraft and aircrew by the 552nd Air Control Wing for the maritime tracking test.
- AFOTEC started suitability data collection with the first operational E-3G version 3.0 during 4QFY15 and will continue through 4QFY16 until the required mission computing operating hours are collected.
- During 2QFY16, AFOTEC conducted a cold weather suitability assessment with the deployment to Eielson AFB, Fairbanks, Alaska. The test was incomplete due to non-Block 40/45-related airframe and surveillance radar failures, which prevented take-off for the planned operational mission. Consequently, the elapsed time for bringing the Block 40/45 mission computing system on-line after a cold weather take-off, could not be measured.
- During 3QFY16, the Air Force conducted a CVPA of E-3G version 3.0 and supporting mission planning, software verification, and training ground systems to assess the system's performance in the presence of a realistic cyber threat.
- During 3QFY16, AFOTEC, with support of the 552nd Air Control Wing, conducted a test over the Gulf of Mexico to characterize E-3G maritime surveillance tracking performance. The comparative test employed a legacy E-3 Block 30/35 and an E-3G version 3.0 conducting surveillance of the same overwater track production area.
- AFOTEC observed and collected data during a 3-week hot weather (daytime temperatures in excess of 110 degrees Fahrenheit) deployment to a Red Flag Large Force Exercise conducted from Nellis AFB, Nevada. To assess operational employment, this test included two E-3G version 3.0 aircraft and Deployable Ground Support System version 3.0—downsized system with more computing capacity—to provide mission planning, rehearsal, and post-mission recording review.
- The Air Force Program Executive Officer (PEO) did not certify the system as "ready for Follow-On Operational Test and Evaluation (FOT&E)" after AFOTEC highlighted deficiencies observed during IOT&E and other events that had not been resolved. The PEO requested AFOTEC utilize the data collected during the Large Force Exercise Red Flag 16-3 to identify deficiencies to be corrected prior to any re-planned FOT&E of Block 40/45.

Assessment

- Observations and emerging results from the FY16 tests indicate that the E-3G version 3.0 has difficulty in combining various on- and off-board sensor data into a coherent single track on a consistent basis. Analysis of air and maritime and ESM sensors to assess and characterize current system performance for single track is ongoing.
- DOT&E could not collect data on E-3G mission computing start time and operating capability during cold weather operations due to aircraft mission cancellations. Additionally, the Deployable Ground System was not available to be deployed to the cold weather operating base. This metric remains unresolved.
- Based on the data collected during the 3-week cybersecurity vulnerability test, the E-3G version 3.0 and supporting Block 40/45 ground systems are highly vulnerable to cyber threats and not survivable.
- Block 40/45 tracking of sensed maritime objects, ships, and platforms, is less effective than the predecessor Block 30/35

aircraft, although both systems demonstrated deficiencies compared to truth data supplied by the Coast Guard.

- The E-3G version 3.0 hardware reliability trend indicates it may meet the post-IOT&E revised threshold requirement for hardware mean time between failure. System deficiency reports and software performance are being reviewed and compared with the revised threshold requirement for software reliability. The ESM sub-system, which experienced some hardware and software modification for Block 40/45, is not reliable due to a combination of legacy, built-in test false alarm, and Block 40/45 problems.
- Insufficient cooling resulting in Deployable Ground System version 1.0 overheating and failure was a critical deficiency identified during the operational deployment to the Caribbean Sea. In contrast, the Deployable Ground System version 3.0 performed well while deployed to Nellis AFB for the Red Flag Exercise and relying on room-modified, dedicated air conditioning ducts. It experienced only one required reboot during the 3-week deployment.
- The E-3G demonstrated several operational deficiencies during Red Flag Large Force Exercise, including inaccurate track quality data processing and inconsistent IFF response displays to the operator.
- Due to the program deficiencies and the PEO's decision to not certify AWACS Block 40/45 as "ready for FOT&E," AWACS Block 40/45 is delayed approximately 2 years while the program manager works to develop resolutions.

Recommendations

- Status of Previous Recommendations: The Air Force has satisfactorily addressed one of the previous recommendations. The Air Force still needs to:
  1. Complete and update aircrew and maintenance checklists and technical orders to address the new failure modes discovered during IOT&E.
  2. Modify the mission computing software and refine technician training to reduce the incidence of induced critical failures during Block 40/45 mission computing startup.
  3. Develop software modifications to improve aircrew ability to control the automated tracking capability.
  4. Review and update the planned training syllabus for both aircrew and maintenance personnel with information learned during the IOT&E.
  5. Conduct FOT&E of Block 40/45 using the first Block 40/45 configuration that will be installed on more than two aircraft. The FOT&E should include an operationally representative deployment in a stressful tracking and combat identification environment.
- FY16 Recommendations. The Air Force should:
  1. Identify the Block 40/45 mission computing hardware and software for E-3G aircraft and ground configurations for the new FOT&E and update the Test and Evaluation Master Plan accordingly to include a description of the planned verification of correction of deficiencies.
  2. Plan to conduct a second CVPA and a cybersecurity Adversarial Assessment as part of the new FOT&E.
  3. Plan to test the integration of new E-3 developmental communications and combat identification capabilities, including Next Generation IFF interrogation system, E-3 AWACS Radar Electronic Protection, Internet Protocol Enabled Communications, Combat Identification (also known as System R), and Communications Network Upgrade, with the Block 40/45 mission computing system and Primary AWACS Display (as appropriate) as part of the FOT&E.
  4. Plan to complete the test of mission computing during cold weather employment.

F-22A Advanced Tactical Fighter

Executive Summary

- F-22A Update 5 combines an aircraft Operational Flight Program (OFP) software suite upgrade providing radar enhancements and Ground Collision Avoidance System software with the integration of limited AIM-9X Block 1 air-to-air missile capabilities. The Air Force Air Combat Command completed a Force Development Evaluation (FDE) of these capabilities in 1QFY16, and the operationally effective system was fielded to F-22A units. Full AIM-9X Block 1 and Block 2 integration will be completed in F-22A Increment 3.2B.
- F-22A Increment 3.2B is a separate Major Defense Acquisition Program modernization effort intended to integrate AIM-120D and AIM-9X missile systems; an Enhanced Stores Management System (ESMS) for weapons integration and employment improvements; Intra-Flight Data Link (IFDL) improvements and electronic protection enhancements; improved emitter geolocation capability; and a Common Weapon Employment Zone for air-to-air missile employment.
  - Increment 3.2B developmental testing experienced delays in FY15 due to additional unplanned regression testing for earlier Increment 3.2A and Update 5 OFP software development efforts and related competition for limited developmental test resources.
  - Increment 3.2B developmental testing continued throughout FY16 but experienced delays due to software stability and performance shortfalls.
    - In-flight cockpit display blanking and ESMS functionality deficiencies resulted in flight safety operating restrictions, and required additional unanticipated OFP software releases and regression testing. Consequently, the planned Air Force Milestone C decision slipped from March to August 2016.
    - At Milestone C, the Air Force authorized the procurement of 35 of 71 planned hardware kits through low-rate initial production (LRIP). The Air Force does not plan to procure the remaining LRIP kits until it confirms progress in resolving the deficiencies noted in FY16.
    - Flight testing through September 2016 showed improvement with cockpit display stability; however, ESMS deficiencies persisted in the software OFP. As of the end of FY16, investigative efforts had not fully ruled out the possible need for system hardware design changes.
  - Given the limited development progress in FY16, it is unlikely that Increment 3.2B developmental testing will complete as planned at the end of April 2017, or that IOT&E will begin as planned in August 2017.

System

- The F-22A is an air-superiority fighter that combines low observability to threat radars, sustained high speed, and integrated avionics sensors.
- Low observability reduces threat capability to engage F-22As with current adversary weapons.
- The aircraft maintains supersonic speeds without the use of an afterburner.
- Avionics that fuse information from the Active Electronically Scanned Array radar, other sensors, and data linked information for the pilot enable employment of medium- and short-range air-to-air missiles, guns, and air-to-ground munitions.
- The Air Force intended the F-22A to be more reliable and easier to maintain than legacy fighter aircraft.
- F-22A air-to-air weapons are the AIM-120C/D radar-guided missile, the AIM-9M/X infrared-guided missile, and the M61A1 20 mm gun.
- F-22A air-to-ground precision strike capability consists of the 1,000-pound Joint Direct Attack Munition and the 250-pound Small Diameter Bomb Increment 1.
- The F-22A program delivers capability in increments. Incremental Enhanced Global Strike modernization efforts include the following current and near-term modernization efforts:
  - Increment 3.1 provides enhanced air-to-ground mission capability, to include geolocation of selected emitters, electronic attack, air-to-ground synthetic aperture radar mapping and designation of surface targets, and Small

Diameter Bomb integration. Increment 3.1 is currently fielded in operational F-22A units.
- Increment 3.2A is a software-only upgrade providing improved electronic protection, Link 16 Receive, and combat identification capabilities. Increment 3.2A is a modernization effort within the scope of the F-22A Advanced Tactical Fighter baseline acquisition program of record and is currently fielded in operational F 22A units.
- Update 5 combines an OFP upgrade providing software driven radar enhancements, Ground Collision Avoidance System software, and the incorporation of limited AIM-9X capabilities. Update 5 OFP FDE testing completed in 1QFY16. The Update 5 OFP is currently fielded in operational F-22A units.
- Increment 3.2B is a separate Major Defense Acquisition Program modernization effort intended to integrate AIM-120D and AIM-9X missile systems; an ESMS for weapons integration and employment improvements; IFDL and electronic protection enhancements; improved emitter geolocation capability; and integration of a Common Weapon Employment Zone for air-to-air missiles employed by the F-22A. The Increment 3.2B IOT&E is currently planned for 4QFY17.

Mission

Commanders will use units equipped with the F-22A to:
- Provide air superiority over friendly and non-permissive, contested enemy territory
- Defend friendly forces against fighter, bomber, or cruise missile attack
- Escort friendly air forces into enemy territory
- Provide air-to-ground capability for counter-air, strategic attack, counter-land, and enemy air defense suppression missions

Major Contractor

Lockheed Martin Aeronautics Company – Fort Worth, Texas

Activity
- The Air Force conducted all testing in accordance with the DOT&E-approved Test and Evaluation Master Plan and Update 5 FDE plan.
- Air Force Air Combat Command completed an FDE of the Update 5 OFP software suite in 1QFY16. Operational flight testing was executed in three phases: assessments of new capabilities and tactics, techniques, and procedures (TTP) development; missionized scenarios to evaluate Update 5 capabilities and assess/refine derived TTPs in a tactical environment; and live fire weapons employment of the AIM-9X. Update 5 capabilities were fielded to operational F-22A units in FY16.
- Increment 3.2B developmental testing continued throughout FY16 but experienced delays due to software stability and performance shortfalls. The Air Force-planned Milestone C decision slipped from March to August 2016. At Milestone C, the Air Force authorized the procurement of 35 of 71 planned hardware kits through LRIP.

Assessment
- The F-22 Update 5 OFP software suite enhancements and limited AIM-9X Block 1 integration are operationally effective. Full AIM-9X Block 1 and 2 missile integration remains to be tested in Increment 3.2B IOT&E. Update 5 further corrected some of the software deficiencies noted in FY15 Increment 3.2A operational testing.
- F-22 Increment 3.2B developmental testing revealed flight safety and system performance shortfalls and experienced delays due to software stability in FY16.
  - The program experienced in-flight cockpit display blanking occurrences for which root cause fault analysis in still ongoing. Flight testing through September 2016 showed improvement with cockpit display stability.
  - The Increment 3.2B ESMS functionality as tested through the end of FY16 did not ensure proper weapons bay door and missile launcher positions, resulting in uncommanded and uncontrollable weapons bay door positions and cycling in f1ight. As with the display blanking problem, ESMS door shortfalls led to additional flight safety restrictions.
    - ESMS deficiencies persisted in the software OFP version flown through the end of September 2016. At the end of FY16, investigative efforts had not yet ruled out the possible need for system hardware design changes. Due to these problems, modification of the remaining three operational test aircraft was delayed until 1QFY17.
    - Delayed modification of the entire nine-aircraft test fleet hinders the program's ability to conduct four-ship test missions, which are needed to vet key Increment 3.2B capabilities and complete developmental testing within the scope of the Air Force's schedule.
  - Although the program has demonstrated some elements of each of the combat capability candidates in laboratory and flight testing, as of the end of September 2016 numerous performance shortfalls exist across the scope of the intended enhancements, and a substantial volume of developmental testing remains to be accomplished.
- The DOT&E November 2015 FOT&E report highlighted F-22A software reliability and performance problems realized in the F-22A Increment 3.2A software suite. In that report, DOT&E cautioned that F-22 modernization efforts risked potentially unacceptable software reliability and associated performance shortfalls unless the Air Force focused concerted efforts on software reliability improvements. Thus far, Increment 3.2B performance and reliability had not shown such improvements.

- F-22A modernization increments and development schedules remain tightly coupled, with little margin for unanticipated regression testing and correction of critical deficiencies when discovered in operational testing. To date, Increment 3.2B developmental testing has experienced several delays due to additional unplanned regression testing for Increment 3.2A and Update 5 OFP efforts in 2015, competition for limited test resources, and problems with Increment 3.2B display blanking and ESMS. These factors contributed to a delayed Increment 3.2B Milestone C decision. Given the limited development progress in FY16, it is unlikely that associated developmental testing will complete as planned at the end of April 2017, or that IOT&E will begin as planned in August 2017.
- In FY15, DOT&E highlighted that integration of the AIM-120D weapon model into the Advanced Combat Simulator (ACS) presented a risk to the Increment 3.2B program's ability to begin scheduled FY17 IOT&E on time. In FY16, delivery of the Raytheon AIM-120D model to Lockheed Martin for incorporation into the ACS remained a risk to the currently planned IOT&E schedule.
- In FY16, the Air Force initiated action to establish a comprehensive strategy for evaluating the cybersecurity vulnerabilities of the F-22 weapon system across the span of projected modernization efforts. Specific strategy details remain to be incorporated into forthcoming F-22 modernization efforts.

Recommendations

- Status of Previous Recommendations. The Air Force continues to address previous recommendations; avionics stability shortfalls remain to be evaluated in the scope of Increment 3.2B IOT&E.
- FY16 Recommendations. The Air Force should:
  1. Correct performance deficiencies and software anomalies associated with Increment 3.2B before proceeding to IOT&E.
  2. Reassess the Increment 3.2B development schedule based on the risks of successful completion due to performance shortfalls realized to date, and ensure the program has adequate resources to complete and deliver the capabilities required by the Air Force with the avionics stability necessary for these capabilities to be operationally effective and suitable.
  3. Continue to improve F-22A avionics software stability to support operational mission execution needs.
  4. Ensure the adequacy of the force structure and schedule margins necessary to support F-22A modernization efforts.

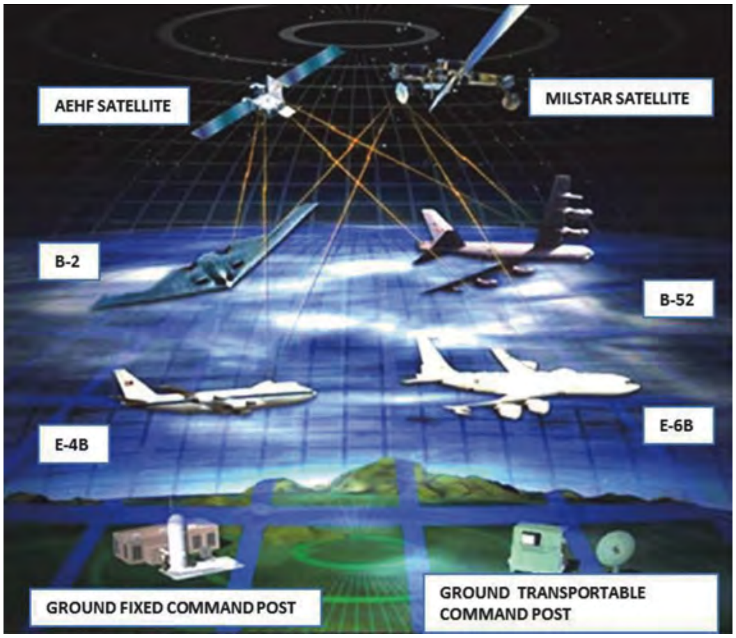
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)

Executive Summary

- On July 16, 2016, USD(AT&L) approved the procurement of 12 antenna modification kits for installation with the Family of Advanced Beyond Line-of-Sight Terminals (FAB-T) Command Post Terminals (CPTs). These modification kits are in addition to the 10 antenna modification kits USD(AT&L) authorized in September 2015 for low-rate initial production. The additional modification kits allow the program to keep in synchronization with airborne depot maintenance schedules and fielding of Initial Operational Capabilities.
- The Air Force's 46th Test Squadron (46 TS) conducted Nuclear Command, Control, and Communications (NC3) developmental testing from March 8 – 11, 2016, with 2 FAB-Ts and 13 cooperating Extremely High Frequency (EHF) terminals.
- The FAB-T Program Office conducted system-level functional qualification testing on the ground-transportable terminal antenna from February through March 2016. The program manager plans to conduct environmental qualification testing on the ground-transportable antenna from September through December 2016.
- The IOT&E has slipped from 4QFY17 to 1QFY18 due to delays in developmental testing and the lead time needed to integrate production-representative terminals required for the operational test at user ground-fixed sites and in ground-transportable platforms.
- The Airborne CPT (ACPT) demonstrated low reliability in the FY15 operational assessment (OA), and if not improved, increases risk to the DOD's Airborne Command Post ability to command and control strategic networks when needed. The program manager updated the reliability growth plan based on the FY15 OA results and OSD staff comments; however, the majority of reliability tracking hours occur after the planned IOT&E. Additionally, the preponderance of the planned hours for the ACPT originate from system integration labs that are not operationally representative of the dynamics experienced in an aircraft. The non-representative environment is unlikely to reveal additional terminal failure modes and may result in additional failure modes being discovered in the IOT&E or during operations.

System

- FAB-T consists of ground and aircraft communication terminals with two terminal types—CPTs and Force Element Terminals (FETs). FAB-T is part of the terminal and control segments of the Advanced EHF (AEHF) satellite system and is designed to operate with AEHF Low Data Rate (75 – 2,400 bits per second (bps)) and Extended Data Rate (up to 8.192 Megabits per second) waveforms.



- The CPT is intended to replace existing airborne (E-4B and E-6B), ground-fixed, and ground-transportable Milstar CPTs. The CPT will include satellite and network control functions, end-user telecommunication device interfaces, and the ability to operate the terminal from a distant location using a remote node.
- The FET is intended to be installed in airborne force elements (B-2, B-52, and RC-135). The FET is a program requirement but is currently neither funded nor on contract for development and production.

Mission

- The President, the SECDEF, Combatant Commanders, and supporting Air Force component forces will use FAB-T to provide strategic nuclear and non-nuclear command and control with EHF, wideband, protected, and survivable communications terminals for beyond line-of-sight communications.
- U.S. Strategic Command will use the FAB-T to perform satellite telemetry, tracking, and commanding functions for the AEHF constellation, including management of the satellites, communication networks, and cryptologic keys.

Major Contractor

Raytheon Net-Centric Systems – Marlborough, Massachusetts

Activity

- During the 2015 OA, the ACPT demonstrated a Mean Time Between Critical Failure of 131.2 hours against a threshold requirement of 665 hours.
- The program manager is executing the developmental test program in accordance with the DOT&E-approved Test and Evaluation Master Plan in preparation for the planned IOT&E.
- At the September 1, 2015, Milestone C decision review, USD(AT&L) directed the program manager to work with DOT&E, the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, and the Deputy Assistant Secretary of Defense for Systems Engineering to determine the appropriate amount of reliability growth testing for the next phase of the program. The October 26, 2015, Acquisition Decision Memorandum tasked the program manager to deliver a plan to USD(AT&L) within 60 days for achieving and verifying the stated reliability requirements.
- The contractor developed Block-2 software and completed software qualification testing in December 2015. Block-2 software is designed to provide FAB-T the capability to perform satellite control functions.
- The 46 TS conducted NC3 developmental testing from March 8 – 11, 2016, with 2 FAB-Ts and 13 cooperating EHF terminals. The NC3 developmental testing employed FAB-T Engineering Development Model terminals.
- The 46 TS conducted an initial satellite control developmental test dry run using an Engineering Development Model terminal from April 4 – 8, 2016, at 4th Satellite Operations Squadron (4 SOPS) on Schriever AFB, Colorado. The program manager discovered integration problems and terminal function anomalies when integrating the satellite control terminal at 4 SOPS in preparation for initial satellite control developmental testing. The program manager postponed the test event pending resolution of integration problems and system anomalies. The program manager resolved the problems and conducted the initial satellite control test from September 8 – 9, 2016.
- The FAB-T Program Office conducted system-level functional qualification testing on the new ground-transportable terminal antenna from February through March 2016. The program manager plans to conduct environmental qualification testing on the ground-transportable antenna from September through December 2016.
- The contractor is developing a new airborne terminal antenna to replace the modified legacy antenna to improve reliability. The program manager plans to conduct environmental qualification testing on the new airborne antenna from September through December 2016.
- On July 16, 2016, USD(AT&L) approved the procurement of 12 antenna modification kits for installation with FAB-T CPTs. These modification kits are in addition to the 10 antenna modification kits USD(AT&L) authorized in September 2015 for low-rate initial production. The additional modification kits allow the program to keep in synchronization with airborne depot maintenance schedules and fielding of Initial Operational Capabilities.

Assessment

- The ACPT demonstrated low reliability in the FY15 OA and, if not improved, increases risk to the DOD's Airborne Command Post ability to command and control strategic networks when needed. The program manager updated the reliability growth plan based on the FY15 OA results and OSD staff comments; however, the majority of reliability tracking hours occur after the planned IOT&E. Additionally, the preponderance of the planned hours for the ACPT originate from system integration labs that are not operationally representative of the dynamics experienced in high-performance aircraft. The non-representative environment is unlikely to reveal additional terminal failure modes and may result in additional failure modes being discovered in the IOT&E or during operations. An Air Force-approved FAB-T reliability plan is still in development and has not been submitted to USD(AT&L).
- The 46 TS's NC3 developmental testing used tester personnel as operators and FAB-T terminals that were not production representative. The testing emulated operational networks and demonstrated interoperability between EHF terminals anticipated to operate in NC3 networks. The NC3 developmental testing provided initial risk reduction and problem identification but needs to be more operationally realistic to provide data for operational test use. The Program Office plans additional NC3 developmental testing in 2QFY17 using production-representative terminals to further reduce the risk of poor IOT&E performance and to achieve U.S. Strategic Command certification.
- The 46 TS's satellite control developmental testing employed testers as operators and used a non-production-representative FAB-T terminal. The test had limited objectives but provided the program manager with good risk reduction for an initial test event. The program manager plans for additional, more operationally realistic satellite control testing in preparation for IOT&E.
- The contractor experienced problems developing the new airborne antenna and with ground-transportable antenna servo control system integration. Completion of developmental testing on the fixed-price development effort is taking longer than planned due to cost pressures that limit test personnel and test assets.
- The IOT&E has slipped from 4QFY17 to 1QFY18 due to delays in developmental testing and the lead time needed to integrate production-representative terminals required for the operational test at user ground-fixed sites and in ground-transportable platforms.

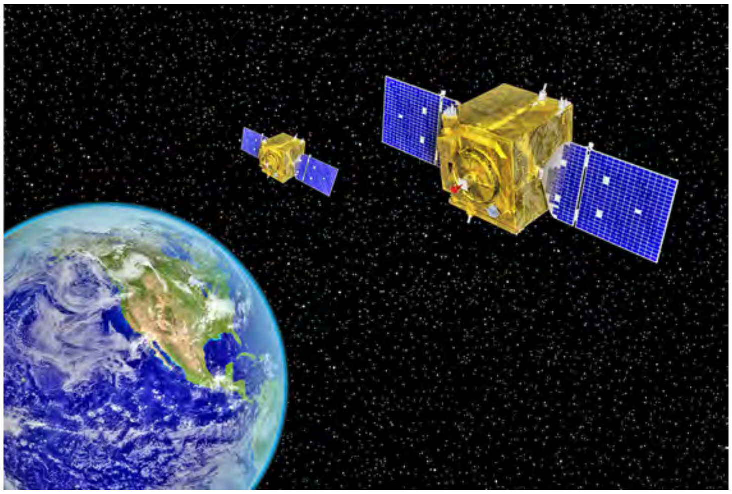
Recommendations

- Status of Previous Recommendations. The Air Force has addressed the previous three recommendations.
- FY16 Recommendation.
  1. The Air Force should continue to use reliability growth test periods to surface more failure modes and correct them to grow reliability and confidence in system performance prior to IOT&E.

Geosynchronous Space Situational Awareness Program (GSSAP)

Executive Summary

- The Air Force operationally accepted and declared Initial Operational Capability (IOC) for the Geosynchronous Space Situational Awareness Program (GSSAP) on September 29, 2015.
- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted IOT&E for GSSAP from August 2015 to January 2016 in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and operational test plan.
- Operational testing of GSSAP was adequate to support an initial but incomplete evaluation of the system's operational effectiveness, suitability, and survivability. The Air Force should conduct FOT&E with adequate threat representation and statistical rigor to resolve unassessed, inconclusive, and shortfall measures from IOT&E.
- GSSAP is effective for some intended operations, but not for others. GSSAP is not suitable due to the inadequacy of operator training and training systems, and dependence on other mission systems with reliability and availability shortfalls. GSSAP survivability is inconclusive.



System

- GSSAP is a space-based, space situational awareness (SSA) capability operating in near-geosynchronous orbit, supporting U.S. Strategic Command (USSTRATCOM) SSA operations as a dedicated Space Surveillance Network sensor.
- The GSSAP system consists of satellites and a ground segment that controls the satellites and receives and processes GSSAP mission data.

Mission

- The 1st Space Operations Squadron, of the Air Force Space Command's 50th Space Wing at Schriever AFB, Colorado, employs GSSAP to satisfy SSA mission tasking from USSTRATCOM's Joint Functional Component Command for Space.
- GSSAP is intended to track and characterize man-made orbiting resident space objects at and near the 22,236 mile (35,786 km) geosynchronous orbit altitude, to contribute to timely and accurate resident space object orbit predictions, knowledge of the geosynchronous orbit environment, and safety of space flight through satellite collision avoidance.

Major Contractor

Orbital ATK – Dulles, Virginia

Activity

- The Air Force operationally accepted and declared IOC for GSSAP on September 29, 2015.
- AFOTEC conducted IOT&E for GSSAP from August 2015 to January 2016 in accordance with the DOT&E-approved TEMP and operational test plan.
- Prior to the IOT&E, the Air Force conducted developmental T&E from August 2014 to July 2015, and integrated T&E from July 2015 to August 2015. In order to decrease the delay from launch to operational availability and to preserve spacecraft operational lifespan, with prior DOT&E approval, AFOTEC used data collected during both developmental and integrated T&E in its OT&E analysis and report.

Assessment

- Operational testing of GSSAP was adequate to support an initial but incomplete evaluation of the system's operational effectiveness, suitability, and survivability. The Air Force should conduct FOT&E with adequate threat representation and statistical rigor to resolve unassessed, inconclusive, and shortfall measures from IOT&E.

- GSSAP is effective for some intended operations, but not for others. GSSAP is not suitable due to the inadequacy of operator training and training systems, and dependence on other mission systems with reliability and availability shortfalls. GSSAP survivability is inconclusive.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Air Force should:
  1. Conduct FOT&E with adequate threat representation and statistical rigor to resolve unassessed, inconclusive, and shortfall measures from IOT&E.
  2. Address the recommendations detailed in the classified DOT&E report.

Global Broadcast Service (GBS) System

1 – Global Broadcast Service Operations Center
2 – Defense Enterprise Computing Center
3 – Primary Injection Point
4 – Transportable Ground Receive Suite
5 – Rucksack Portable Receive Suite
6 – Shipboard Receive Suite
7 – Subsurface Receive Suite
8 – Suitcase Portable Receive Suite

Executive Summary

- The program manager is developing the Global Broadcast Service (GBS) Phase-IV capability that includes an upgraded Transportable Ground Receive Suite (TGRS), new Rucksack Portable Receive Suite (RPRS), new Suitcase Portable Receive Suite (SPRS), and integration of the Digital Video Broadcasting – Satellite – Second Generation (DVB-S2) waveform that should provide more efficient use of available satellite bandwidth.
- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted FOT&E-1 from May 25 through June 30, 2016, with participation from the Army Test and Evaluation Command, Marine Corps Operational Test and Evaluation Activity, and the Navy's Commander, Operational Test and Evaluation Force. FOT&E-1 included operators from the Air Force, Marine Corps, and Army operating and maintaining receive suites at Robins AFB, Georgia. The USS *Carl Vinson* (San Diego, California) and USS *Santa Fe* (Pearl Harbor, Hawaii) participated for the Navy, communicating over the Wideband Global Satellite Communications (WGS) system.
- The GBS receive suites are operationally effective in providing a continuous flow of high-speed, high-volume, multimedia communications for deployed and garrisoned forces.
- The GBS is not survivable against internal or external cybersecurity threats. The Army Threat Systems Management Office found 17 cybersecurity vulnerabilities on the GBS system that could be exploited by potential adversaries.
- The GBS receive suites are not suitable because the system did not demonstrate that it could meet reliability and maintenance repair times, and the documentation lacked adequate troubleshooting procedures. The systems can be made suitable once corrective actions to improve cable durability, system shutdowns, and technical documentation are made and verified. The program manager is in the process of updating technical orders and technical manuals, performing root cause analysis, and implementing corrective actions.

System

- The GBS is a satellite-based broadcast system providing near-worldwide, high-capacity, one-way transmission of operational military data.
- The GBS system consists of three segments:
  - The space segment includes GBS transponders on WGS, Ultra High Frequency Follow-On (UFO) satellites, and an additional government-leased commercial satellite capability to meet operational demand.
  - The transmit segment consists of the GBS Operations Center and Satellite Broadcast Manager (SBM). The GBS Operations Center, located at Peterson AFB, Colorado, remotely creates and manages the GBS broadcast through the primary and alternate SBM located at Oklahoma City, Oklahoma, and Mechanicsburg, Pennsylvania, respectively. The SBM receives data and video products from a variety of sources and packages that source material into a satellite broadcast. The SBM interfaces through DOD Teleport sites for the WGS satellites and fixed Primary Injection Points for the UFO satellites and commercial satellites.
  - The receive segment consists of ground- and sea-based mobile terminals that extract the appropriate information for distribution to the end users within selected areas of operation. The receive suite configurations include the TGRS, RPRS, SPRS, Shipboard Receive Suite, and the Subsurface Receive Suite.

Mission

- Combatant commanders and operational forces worldwide use GBS to provide a continuous high-speed and high

volume flow of data, audio, imagery, and video at multiple classification levels for sustained operations.
- Commanders use the GBS capability to provide intelligence and battlespace weather information, increasing the joint operations mission data available to deployed and garrisoned military forces across the globe.

Major Contractor
- General Dynamics C4 Systems – Taunton, Massachusetts
- AQYR Technologies – Hollis, New Hampshire

Activity
- The program manager is developing GBS Phase-IV capability that includes an upgraded TGRS, new RPRS, new SPRS, and integration of the DVB-S2 waveform that provides more efficient use of available satellite bandwidth.
- On November 13, 2014, the DOD Chief Information Officer instructed the Director, Defense Information Systems Agency to redirect the acquisition strategy of the Joint Internet Protocol Modem from a development program to a commercial off-the-shelf solution. The commercial solution is named the Enterprise Satellite Communications (SATCOM) Gateway Modem. The GBS program's Phase-V is intended to integrate the Enterprise SATCOM Gateway Modem in the GBS architecture to provide waveform protection through implementation of transmission security to prevent potential communications traffic analysis by adversaries.
- The GBS program manager, AFOTEC, and Service representatives updated the GBS Test and Evaluation Master Plan (TEMP) to include the Phase-IV capabilities and testing. DOT&E approved the TEMP update on March 21, 2016.
- The Air Force's 46th Test Squadron (46 TS) conducted a government Developmental Test and Evaluation 2 (DT&E-2) from October 19 through November 20, 2015, at Robins AFB, Georgia, and Naval Base San Diego, California, to assess the end-to-end broadcast and receive capabilities of the GBS receive suites using the DVB-S2 waveform.
- The 46 TS conducted a government DT&E-2 regression test from February 16 through March 18, 2016, at Robins AFB, Naval Base San Diego, and Pearl Harbor, Hawaii, to assess the end-to-end broadcast and receive capabilities of the GBS receive suites running the new GBS receive suite software. The GBS Program Manager delivered updated GBS receive suite software and technical manuals prior to the 46 TS DT&E regression test.
- The Air Force's 92nd Cyberspace Operations Squadron conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) from February 21 through March 12, 2016, during the program manager's developmental test period.
- AFOTEC conducted FOT&E-1 from May 25 through June 30, 2016, with participation from the Army Test and Evaluation Command, Marine Corps Operational Test and Evaluation Activity, and the Navy's Commander, Operational Test and Evaluation Force. FOT&E-1 included operators from the Air Force, Marine Corps, and Army operating and maintaining receive suites at Robins AFB. The USS *Carl Vinson* and USS *Santa Fe* participated for the Navy, communicating over WGS. AFOTEC conducted FOT&E-1 in accordance with the DOT&E-approved TEMP and test plan. The FOT&E-1 start date was preceded by a dry run period from May 16 – 30, 2016. Prior to the operational test, the program manager provided updated GBS operator manuals.
- The Army's Threat Systems Management Office conducted a cybersecurity Adversarial Assessment on the GBS system from June 1 – 20, 2016, during AFOTEC's FOT&E-1.
- DOT&E submitted a report for an Air Force Space Commander operational acceptance decision planned for November 2016.

Assessment
- The 46 TS conducted DT&E-2 to evaluate the receive capabilities of the TGRS, RPRS, and SPRS over the DVB-S2 broadcast and to document and report discovered deficiencies for the program manager to correct prior to the DT&E-2 regression test. The GBS successfully completed 26 of 29 test objectives. The GBS system did not verify three reliability objectives because the allotted test time was insufficient to provide data for evaluating reliability with statistical confidence. The testers also found that the receive suite technical orders troubleshooting steps were incomplete or inaccurate. The incorrect and missing procedures led to delays in users resolving problems and restoring the systems to operation.
- The DT&E-2 regression test demonstrated that the receive suites correctly received and processed data and video, but testers and users noted problems with reliability. Once set up, the GBS system is intended to operate without operator attention for a minimum of 24 hours, and up to 83 days. The reliability problems cause operators to intervene to restore the system to operations, diverting them from other mission needs. The updated documentation for troubleshooting still lacked clarity, with missing or incomplete troubleshooting steps.
- During the CVPA, the 92nd Cyberspace Operations Squadron discovered 54 potential vulnerabilities and compliance findings with the GBS system. The program manager corrected some of the discovered potential vulnerabilities and compliance findings, but many remained uncorrected or successfully mitigated in the operational test.
- The GBS receive suites are operationally effective in providing a continuous flow of high-speed, high-volume, multimedia communications for deployed and garrisoned forces.

- The GBS is not survivable against internal or external cybersecurity threats. The Army Threat Systems Management Office found 17 vulnerabilities on the GBS system that could be exploited by potential adversaries.
- The GBS receive suites were not suitable because the system did not demonstrate it could meet reliability and maintenance repair times, and documentation lacked adequate troubleshooting procedures. The systems can be made suitable once corrective actions to improve cable durability, system shutdowns, and technical documentation are made and verified. The program manager is in the process of updating technical orders and technical manuals, performing root cause analysis, and implementing corrective actions.

Recommendations

- Status of Previous Recommendations. The Air Force has addressed all previous recommendations.
- FY16 Recommendations. The Air Force should:
  1. Correct the problems with the cables, system shutdowns, and documentation, and verify the corrections in the GBS operational trial period and FOT&E-2.
  2. Correct the cybersecurity vulnerabilities and conduct a CVPA and Adversarial Assessment in the next operational test.

Global Positioning System (GPS) Enterprise

Executive Summary

- The Air Force conducted significant developmental test and evaluation (DT&E) for all three GPS enterprise segments (space, control, and user) in 2016, but did not conduct any operational testing for the GPS enterprise in 2016. DT&E included GPS III thermal vacuum test and post-thermal vacuum system performance and electromagnetic compatibility testing, Next Generation Operational Control System (OCX) Launch Checkout System DT&E, and the second of five phases of DT&E for Military GPS User Equipment (MGUE) Increment 1.
- Expected operational testing dates for all segments have been delayed from dates listed in prior DOT&E Annual Reports and the Enterprise Test and Evaluation Master Plan (ETEMP), approved by DOT&E in March 2012.
- The ETEMP requires an update to reflect test strategy, schedule, and resource changes due to segment delays, acquisition strategy changes, policy and threat changes, and the initiation of the GPS III Contingency Operations (COps) program. An updated ETEMP is in Military Service coordination with formal OSD review expected early 2017.
- Delays to the OCX have worsened since the FY14 DOT&E Annual Report, and the post-Nunn-McCurdy recertified, restructured OCX program cannot deliver OCX Block 1 in time for operational constellation sustainment. The Air Force has initiated the COps program to enable employment of GPS III, using a subset of their capabilities, satellites to sustain the operational constellation prior to OCX availability.
- Significant GPS Enterprise risks remain:
  - Ongoing risk that OT&E of GPS III satellites will not occur until after as many as eight of the satellites are built and on-orbit, increasing the risk that deficiencies will not be discovered until it is too late to correct them.
  - Ongoing risk that insufficient platform integration will occur in time for the operational assessment (OA) of MGUE Increment 1, jeopardizing acquisition decisions made on the basis of that OA.
  - Ongoing risk that the DOD has not assessed the degree to which designated Lead Platforms for MGUE Increment 1 cover the range of operational factors and integration challenges for the complete portfolio of DOD programs that will integrate MGUE Increment 1, and that Lead Platform and MGUE Increment 1 limitations will impede the pathfinding value of integration and OT&E on those platforms.
  - Ongoing risk to the integration and fielding of MGUE Increment 1 with the DOD portfolio posed by the lack of a plan for comprehensive risk-reduction integration testing with all platforms, munitions, and platform interfaces expected to integrate MGUE Increment 1.

AFSCN – Air Force Satellite Control Network
GPS IIR – Global Positioning System (GPS) Block II "Replenishment" Satellites
GPS IIR-M – GPS Block II "Replenishment – Modernized" Satellites
GPS IIF – GPS Block II "Follow-On" Satellites
GPS III – GPS Block III Satellites

  - Risk to adequate OT&E of MGUE Increment 1 posed by the apparent gap between the Air Force intent for delivered MGUE Increment 1 functional capabilities and Military Service operational environment-driven performance requirements.
  - Risk to sustainment of the operational GPS constellation posed by inadequate resource prioritization and commitment to ensure successful, low-risk execution of the COps program, and the absence of independent active monitoring of COps development progress.

System

- The GPS enterprise is an Air Force-managed, satellite-based radio navigation system of systems that provides military and civil users accurate position, velocity, and time within the multi-trillion cubic kilometer volume of near-earth space, earth atmosphere, and worldwide earth surface areas.
- The current GPS enterprise consists of three operational segments:
  - Space Segment – The GPS spacecraft constellation consists of a minimum of 24 operational satellites in semi-synchronous orbit. The Air Force has successfully launched 70 GPS satellites and currently operates 31 healthy GPS satellites, comprising Block IIR (1997-2004), Block IIR-M (2005-2009), and Block IIF (2010-present).
  - Control Segment – The GPS control segment consists of primary and backup GPS master control stations, satellite control antennas, a pre-launch satellite compatibility station, and geographically-distributed operational monitoring stations. The current GPS control segment includes the Operational Control System

(OCS)/Architecture Evolution Plan (AEP) supporting (1) operation of GPS Block IIR, IIR-M, and IIF satellites, (2) Selective Availability/Anti-Spoof Module capabilities in U.S. military and authorized Federal and allied military GPS User Equipment, the Launch/Early Orbit, Anomaly Resolution, and Disposal Operations (LADO) system, and the Selective Availability Anti-Spoofing Module (SAASM) Mission Planning System (SMPS).
  - User Segment – There are many versions of military GPS mission receivers fielded on a multitude of operational systems and combat platforms, including the most common Defense Advanced GPS Receivers and embedded Ground-Based GPS Receiver Application Modules (GB-GRAM), numbering in the hundreds of thousands.
- In 2000, the DOD approved initiation of a GPS enterprise modernization effort to include upgrades to all three segments, along with new civil and military signals (M-code). In addition to replenishment of the satellite constellation, this modernization is intended to improve both military and civil signal integrity and service quality in terrain- and geography-impeded environments, as well as in the presence of unintentional and deliberate interference. Modernized GPS enterprise improvements include:
  - Space Segment – GPS III satellites, an Acquisition Category (ACAT) 1D program, have a design life exceeding that of earlier blocks. GPS III satellites are intended to be capable of transmitting a fourth civil signal and higher-powered M-code, as well as all legacy military and civil navigation signals of previous satellite blocks.
  - Control Segment – OCX, an ACAT 1D program to be delivered in three blocks, replaces the current OCS/AEP control segment and LADO, is backward compatible with Block IIR and later satellites, and will interface with modified SMPS versions. OCX is intended to provide significant cybersecurity improvements over OCS, and through OCX Block 0 the ability to launch and check out GPS III satellites, through OCX Block 1 the ability to control GPS Block II and III satellites, and through OCX Block 2 the full control of modernized civil and M-code signals and navigation warfare functions.
  - User Segment – MGUE Increment 1 is an ACAT ID program and Increment 2 is a pre-Major Defense Acquisition Program, expected to be ACAT 1D. MGUE Increment 1 includes the GB-GRAM-Modernized form factor for ground and low-dynamic platforms such as small unmanned aircraft systems, and the GRAM-Standard Electronic Module-E/Modernized for maritime and aviation applications. The MGUE Increment 2 Capability Development Document is in development and presumed to address requirements and applications not addressed by MGUE Increment 1, including handheld, precision-guided munition, and standard space receiver applications.
- Delays in OCX Block I delivery led the Air Force in 2015 to initiate the COps program as a "bridge capability" to enable employment of GPS III satellites, using only legacy signals, for operational constellation sustainment until OCX Block 1 is available.

Mission
- Combatant Commanders, U.S. military forces, allied nations, and various civilian agencies rely on GPS to provide highly accurate, real-time, all-weather, position, navigation, and time information to operational users worldwide. GPS provides force enhancement for combat operations and military forces in the field on a daily basis throughout a wide variety of global strategic, operational, and tactical missions.
- Appropriately equipped military forces will employ modernized GPS capabilities to (1) determine or contribute to their determination of their location and velocity, (2) support precision munitions targeting and employment, and (3) synchronize operations and secure communications in all environments.

Major Contractors
- Space Segment
  - Block IIR/IIR-M/III satellites: Lockheed Martin Space Systems – Denver, Colorado
  - Block IIF satellites: Boeing, Network and Space Systems – El Segundo, California
- Control Segment
  - OCS: Lockheed Martin, Space Systems Division – Colorado Springs, Colorado
  - OCX: Raytheon Company, Intelligence, Information, and Services – Aurora, Colorado
  - COps: Lockheed Martin, Space Systems Division – Colorado Springs, Colorado
- User Segment (MGUE Increment 1)
  - L-3 Communications/Interstate Electronics Corporation – Anaheim, California
  - Raytheon Company, Space and Airborne Systems – El Segundo, California
  - Rockwell Collins – Cedar Rapids, Iowa

Activity
- The Air Force conducted significant DT&E for all three enterprise segments in 2016, including GPS III thermal vacuum test and post-thermal vacuum system performance and electromagnetic compatibility testing, OCX Launch Checkout System DT&E, and the second of five phases of DT&E for MGUE Increment 1. It did not conduct any operational testing for the GPS enterprise in 2016.
- Expected operational testing dates for all three segments have been delayed from dates listed in the current ETEMP approved in March 2012, and in prior DOT&E Annual Reports. Those

schedule changes resulted from development and delivery delays for all segments, as well as from Lead Platform integration-related delays caused or exacerbated by MGUE Increment 1 development delays and management decisions.

- OCX cost and schedule exceedance led to a Nunn-McCurdy Act program review and recertification.
- The Air Force currently expects to conduct operational tests for each GPS segment as follows:
  - The planned OA of MGUE Increment 1 has slipped to late 2017, primarily due to the immaturity of MGUE Increment 1 initial test articles and delayed delivery of follow-on test articles. That planned OA was previously accelerated from late 2016 to late 2015 to support a planned USD(AT&L) combined Milestone B/C decision under an accelerated schedule approved in the MGUE Increment 1 Acquisition Strategy Document (ASD). USD(AT&L) now plans to conduct a Milestone B-only Defense Acquisition Board for MGUE Increment 1 in early 2017, and it is unclear what post-Milestone B or Beyond Low-Rate Initial Production (BLRIP) decisions will occur for MGUE.
  - The planned IOT&E of MGUE Increment 1 has slipped to 2019 through 2020. This IOT&E will involve data gathered during testing in four separate operational utility evaluations (OUEs) of MGUE Increment 1 on the four designated Lead Platforms. The Air Force had previously accelerated the IOT&E from 2021 to 2017, to support the USD(AT&L) planned BLRIP decision for MGUE Increment 1, based on the schedule approved in the MGUE Increment 1 ASD.
  - The planned OUE of OCX Block I has slipped from early 2016, to early 2019, and now to no sooner than mid-2022, with low confidence in that schedule. This OUE was to combine with an OUE of GPS III satellite vehicle (SV)01 to support an Air Force fielding decision for OCX Block 1 and operational acceptance of GPS III SV01.
    - A December 2015 USD(AT&L) Acquisition Decision Memorandum directed a restructure and 24-month extension for OCX Block 1 delivery, to between mid-2021 and mid-2022. Indications of critical cost and schedule breaches led to a June 2016 Secretary of the Air Force Nunn-McCurdy notification for OCX to Congress.
    - In October 2016, USD(AT&L) recertified a restructured OCX program, rescinded the OCX Milestone B, and directed the Air Force to return for a Milestone B Defense Acquisition Board no later than June 30, 2017. The Air Force plans to propose an Acquisition Program Baseline with a mid-2022 delivery of OCX Block 1.
    - The OCX Block 1 delivery and GPS III SV01 delivery and launch are no longer aligned. The initial GPS III OUE, excluding test of modernized signals, will now occur concurrently with the OUE of COps, which must be developed and fielded to allow employment of GPS III satellites with legacy-only capability to sustain the operational constellation of 24 GPS satellites.
  - The COps OUE is currently planned for mid-2019, concurrent with the OUE of GPS III SV01, in support of a Program Executive Officer Space (Commander, Air Force Space and Missile Systems Center) limited fielding decision for COps and a Commander, Air Force Space Command operational acceptance decision for COps.
  - An initial GPS III OUE is currently planned for mid-2019, concurrent with the OUE of COps, in support of a USD(AT&L) limited fielding decision for GPS III SV01 excluding use of modernized GPS signals, and a Commander, Air Force Space Command operational acceptance decision for GPS III SV01, using legacy-only signals. Post-thermal vacuum chamber defect discovery on GPS III SV01 delayed the satellite's availability-for-launch, but it will still likely be ready for launch before the OCX Block 0 control segment will be ready to support GPS III launch and checkout.
  - Multi-Service OT&E (MOT&E) of the modernized GPS enterprise has slipped to an indeterminate date beyond 2022, and will be required after delivery of OCX Block 2-associated navigation warfare and modernized signal and messaging functions, supporting a fielding decision for OCX Block 2 and/or operational acceptance decisions for those capabilities. GPS Enterprise MOT&E was previously planned for 2020, but can occur no earlier than the delivery of OCX Block 2-associated functions.
- Although the GPS Program Office continues to support Service platform program office efforts to incorporate keyed military GPS receivers in their weapons, and the Services have made progress increasing integration of, training with, and reliance on keyed military receivers, the Joint Navigation Warfare Center-compiled data show many DOD weapon systems continue to use non-military receivers and some forces fail to routinely key and train with keyed military receivers.
- The next revision of the GPS ETEMP remains in coordination within the Air Force and Service Operational Test Agencies, and the Air Force plans to submit it for formal OSD review in early 2017. The approved GPS ETEMP is over 4 years old, and is outdated, but revision has been delayed by significant fluctuation in all enterprise segment delivery and availability schedules, as well as the OCX and MGUE acquisition strategies, and initiation of COps.

Assessment

- No OT&E test data are available at this point.
- In the FY14 Annual Report, DOT&E cited concerns identified in DOT&E's November 2014 memorandum to USD(AT&L) regarding sustainment and modernization of GPS capabilities. Those concerns remain valid, with some mitigation:
  1. OCX delays limit adequate, timely OT&E for GPS III satellites prior to extensive procurement and incorporation of the GPS III satellites into the operational constellation.
  2. Deferred platform integration jeopardizes adequate MGUE Increment 1 OA and risks late deficiency discovery.
  3. There is limited pathfinding value to Lead Platform testing compared to the represented portfolio of platforms.
  4. Limiting MGUE integration funding for each Lead Platform to the first available MGUE Increment 1 vendor card risks

limiting post-IOT&E competition and delays to MGUE Increment 1 fielding throughout the DOD portfolio.

5. There is inadequate articulation of program risks. This is being addressed. The Air Force has acknowledged the numerous schedule and performance risks to GPS outlined in this report; mitigation of those risks is incomplete.
6. The program schedules are inaccurate, implausible, and incoherent. This is being addressed. The Air Force has established a plausible schedule for MGUE Increment 1, with the exception of undefined Milestone Decision Authority (MDA) decisions for BLRIP activities on Lead Platforms and non-Lead Platforms. The GPS enterprise schedule appears to better reflect facts-in-being for each segment modernization effort.
7. The Air Force has overstated MGUE development maturity. This point has been demonstrated by the poor performance of initial MGUE Increment 1 test articles during the first phase of government DT&E in late 2015. MGUE Increment 1 has demonstrated marginal technical maturity and platform interoperability improvements to-date.

- In a January 2016 memorandum to the SECDEF, DOT&E identified concerns with the risk to U.S. GPS capability posed by delays to OCX and inadequate prioritization and resource allocation for COps development. DOT&E recommended that the SECDEF direct the Air Force to prioritize resources to ensure successful COps execution and require COps progress reporting in quarterly OCX reports to the Comptroller General, to facilitate active monitoring. The Air Force included cursory information but no detailed COps status in its first two quarterly OCX reports.
- In a January 2016 memorandum to USD(AT&L), DOT&E recommended against approving a combined Milestone B and C for MGUE Increment 1, stated that MGUE Increment 1 testing to-date did not indicate that current designs could be produced and would work, and that MGUE interoperability risk remained substantial and unmitigated. DOT&E further recommended expanded risk-reduction integration testing with all platforms, munitions, and platform interfaces expected to integrate MGUE Increment 1, and completion of DT&E and an adequate OA prior to USD(AT&L)'s Milestone C decision. USD(AT&L) has not approved MGUE Increment 1 Milestones B or C and has postponed until January 2017 the Milestone B Defense Acquisition Board previously scheduled for October 2016. USD(AT&L) has not directed, and the Air Force has not elected to conduct the DOT&E-recommended expanded risk-reduction testing.
- In a July 2016 memorandum to the SECDEF, DOT&E reiterated the urgent need for greater focus on COps, to ensure its availability to sustain GPS operations, and recommended the Air Force prioritize and commit resources to ensure successful, low-risk execution of the COps program and active monitoring of COps development progress. COps remains on DOT&E oversight and has not been placed on USD(AT&L) oversight.
- At the time of this report, the MGUE Increment 1 program is preparing for a Milestone B Defense Acquisition Board review with USD(AT&L). DOT&E concerns include:
  1. The mismatch between the approved MGUE Increment 1 ASD, actual program execution, and the ETEMP-described acquisition and test strategies as well as the need for clarification on planned acquisition decisions. Specifically, DOT&E requires clarity on the criteria and timing of acquisition milestone decisions which will allow MGUE Increment 1 and derived components to be fielded on Lead Platforms and non-Lead Platforms. This is needed in order to recommend an appropriate OT&E strategy to provide assessment in support of fielding decisions.
  2. The absence of a plan to assess MGUE Increment 1 performance across the wide variety of intended interfaces and platforms leaves significant unmitigated integration risk, and therefore fielding cost and schedule risk for the DOD.
  3. An apparent gap between MGUE Increment 1 functional capabilities and Military Service operational requirements. For example, Army requirements for the D3/Stryker's operational environment exceed Air Force-planned MGUE Increment 1 functional capabilities. This jeopardizes the adequacy of MGUE Increment 1 OT&E on the D3/Stryker Lead Platform.
- When the Air Force returns in mid-2017 for the post-Nunn-McCurdy Milestone B Defense Acquisition Board, it plans to propose a mid-2022 delivery of OCX Block 1. The program's ability to deliver OCX Block 1 on that schedule, if possible, will be dependent on the successful execution of several test strategy and test resource changes. These changes include implementation of planned automated software testing, increases in contractor and Program Office skilled software subject matter expertise, and procurement of additional software development and testing environments to address resource constraints within and between GPS segments.
- Additional OT&E of MGUE will be required for non-Lead Platforms integrating MGUE and covering operational and environmental conditions for MGUE not evaluated during planned Lead Platform testing.
- Additional OT&E of all M-code-capable satellite blocks will be required once an M-code-capable control segment and user equipment are available, prior to the operational employment of M-code signals from those satellites. The M-code capabilities of GPS Block IIR, IIR-M, and IIF satellites have not previously been operationally tested, and should be included in OT&E, along with GPS Block III M-code capabilities, once OCX is available to support testing.

Recommendations

- Status of Previous Recommendations. The Air Force has partially addressed the five previous recommendations listed in the FY11 Annual Report:
  1. There has been no opportunity thus far for end-to-end testing of OCX with MGUE receivers, and the ETEMP requires revision to reflect updated planning for the MOT&E of the modernized GPS enterprise, which will address end-to-end testing. The Air Force does not have a plan for adequate integration on representative platforms

to enable timely OT&E in representative environments in support of acquisition and fielding decisions. The Air Force should continue to plan for end-to-end testing of the GPS enterprise, including integration on Lead Platforms and non-Lead Platforms, and DT&E and OT&E in realistic operational environments, in time to support acquisition decisions.

2. The Air Force has improved synchronization of the development of the Space, Control, and User segments, in that descriptions of the effect of delays in each segment upon the GPS enterprise and other segment schedules are more often clearly articulated. Delays in MGUE Increment 1 and OCX Block 1 will result in their delivery after most of the first block of GPS III satellites are built and launched. The Air Force should ensure that status and critical interdependencies of each enterprise segment are well understood, and should promptly assess and disseminate to all stakeholders those predicted enterprise impacts resulting from forecast changes in segment schedules.
3. The revised ETEMP still in Service coordination reflects improvements in planning for comprehensive and realistic cybersecurity testing of the GPS enterprise, although additional revisions will be necessary to reflect GPS segment changes and DOT&E's August 2014 guidance, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs. The Air Force should continue to refine its cybersecurity testing approach to GPS.
4. The Military Services have made progress in emphasizing/enforcing the use of crypto-keyed GPS receivers, but should redouble their efforts, in accordance with Joint Navigation Warfare Center and United States Strategic Command recommendations.
5. The Military Services have made progress in developing concepts of operations and tactics, techniques, and procedures for keying GPS receivers, but that has not translated into use of encrypted receivers for all military operations.

- The Air Force has partially addressed the seven recommendations listed in the FY14 Annual Report:
  1. If COps is delivered as planned, it will support a partial OT&E of the first GPS III satellite, but substantial risk of undiscovered deficiencies will remain until completion of GPS III OT&E when OCX Block 2 is available. The Air Force should still mitigate this risk.
  2. The Air Force now intends to include data from integration and DT&E of MGUE Increment 1 on at least some Lead Platforms in an OA informing as-yet-undetermined MGUE Increment 1 acquisition decisions. The Air Force plans to propose at the next MGUE Defense Acquisition Board adoption of multiple "Technical Requirements Verification" decisions in lieu of a Milestone C decision for the program. The Air Force should still plan for an adequate OA encompassing integration and DT&E on at least one Lead Platform per form factor to inform these acquisition decisions.
  3. The Air Force is continuing the engineering, manufacturing, and development of MGUE Increment 1, and resumed government DT&E in mid-2016, but has no plan or direction to conduct comprehensive integration and interoperability testing on non-Lead Platforms to determine MGUE Increment 1 integration maturity. The Air Force should still plan for and conduct comprehensive risk-reduction integration testing with all platforms, munitions, and platform interfaces expected to integrate MGUE Increment 1.
  4. The Air Force has no plan to assess the degree to which designated Lead Platforms for MGUE Increment 1 cover the range of operational factors and integration challenges for the complete portfolio of DOD platforms each MGUE form factor is intended to support. The Air Force believes the DOD should conduct this assessment, but that it is out of scope for the MGUE program. USD(AT&L) should direct the Air Force or another organization to conduct this assessment.
  5. The Air Force does not plan to ensure each available MGUE Increment 1 vendor solution for a given form factor is integrated with all Lead Platforms for that respective form factor to support adequate MGUE IOT&E. The Air Force has recommended a "first card" strategy, in which each Lead Platform will integrate and complete DT&E and OT&E with the first vendor card available, with no provision for the follow-on integration and testing of the other vendor cards as each becomes available. The Air Force should still pursue an "each card" strategy, integrating and testing each MGUE Increment 1 vendor solution on applicable Lead Platforms as soon as those vendor solutions are available.
  6. The Air Force has identified risks to the GPS enterprise and has articulated plans of action and milestones for the mitigation of some risks, but not all. The Air Force should still identify and articulate mitigation plans for all significant risks to the GPS enterprise, in particular, for the risk that COps will not be delivered in time to support constellation sustainment.
  7. The Air Force has improved the coherence of its GPS enterprise schedule information, but these schedules are not always updated to reflect the most current government estimates, nor caveated to reflect un-validated assumptions. The Air Force should maintain and disseminate coherent, accurate, and timely schedule information for all segments, ensuring the schedules reflect segment interdependencies, most current government estimates, and caveats for un-validated assumptions.
- FY16 Recommendation.
  1. The Air Force should prioritize and commit resources to ensure successful, low-risk execution of the COps program, and ensure active independent monitoring of COps development progress.

Joint Space Operations Center (JSpOC) Mission System (JMS)

Executive Summary

- The Air Force has yet to conduct any OT&E for Joint Space Operations Center (JSpOC) Mission System (JMS) Increment 2, but conducted significant development and developmental testing for JMS Increment 2, Service Packs (SP) 9 and 11 in 2016, including three phases of functional developmental testing for SP9 and developmental cybersecurity assessments.
- The Air Force completed a Critical Change review for JMS Increment 2 in August 2016 due to both schedule and cost increases, and consequently descoped Increment 2 capabilities and deferred final delivery from July 2016 to May 2019. Descoped capabilities no longer being delivered with JMS Increment 2 include the Special Access Program (SAP)-level enclave, automated high-priority tasking, advanced space order of battle tools, and the capability to ingest and process data from non-traditional space situational awareness (SSA) sensors.
- The Air Force is planning an Operational Utility Evaluation (OUE) of JMS Increment 2, SP9 in 2017, following an integrated test and evaluation (IT&E) period, and the developmental testing campaign, which is in progress.
- The Air Force is finalizing a revision to the JMS Test and Evaluation Master Plan (TEMP) to reflect program schedule and content changes, including OT&E for SP11, necessitated by the addition of functional capabilities.
- Delayed interoperability testing between JMS and Space Fence Increment 1 adds risk to cost and delivery schedule for both programs.

System

- JMS is a net-centric, service-oriented architecture of hardware, software, data, and network connectivity that will process, integrate, store, and allow for the compilation, exploitation, sharing, and visualization of SSA sensor data and analysis to support command and control tasking and battle-management decisions for space forces.
- Operational JMS hardware strings and infrastructure are installed at Vandenberg AFB, California, and will be installed at a backup site at Naval Support Facility Dahlgren, Virginia. Additional non-operational instances and partial-instances of JMS are installed for development and developmental testing purposes at a multitude of other sites, including Vandenberg AFB, California, and Space and Naval Warfare Systems Center Pacific at the Point Loma Annex of Naval Support Center San Diego, California.
- JMS net-centric enterprise services, including data visualization, mission applications, and functional queries, are accessible to worldwide users running JMS client software on non-JMS workstations connected through the Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communication System (JWICS) Network.
- JMS will replace legacy Space Defense Operations Center (SPADOC) and space specific portions of the Correlation, Analysis, and Verification of Ephemerides Network (CAVENet) systems.
- The Air Force is developing JMS in two increments.
  - Increment 1 delivered an initial service-oriented architecture infrastructure and user tools, including a client workstation-accessible User Defined Operational Picture that allows access to and analysis of data from legacy systems, integrated collaboration/messaging/data sharing tools, and space order of battle processing.
  - Increment 2 is being developed to deliver mission functionality in three SPs.
    - SP7 delivered updates and additions to Increment 1-delivered hardware and software infrastructure, including servers, space surveillance network (SSN) communications services connectivity, system security and message processing capabilities, and limited space surveillance data processing and visualization tools. SP7 was not operationally tested because it will not replace legacy SPADOC and CAVENet systems nor be used for mission critical functions.
    - SP9 is intended to update and expand JMS hardware and software to perform functions currently performed by SPADOC and CAVENet, with improved accuracy, efficiency, and responsiveness. Those functions include administration and maintenance of the space catalog, orbit determination for resident space objects (RSOs), assessment of conjunctions (collision risk) between

RSOs, and high-accuracy tasking of sensors for orbital safety, threat modeling, and operational decisions.

- SP11 is intended to complete Increment 2 functionality on the Top Secret enclave. SP11 is intended to include the ability to ingest and integrate more highly-classified data, support routine Space Object Identification tasking, and support processing for critical events such as RSO Closely Spaced Operations, breakups, re-entries and de-orbits, launch processing, and processing of uncorrelated tracks. SP11 is also intended to encompass test, training, and exercise capabilities and availability and reliability improvements which had been planned for delivery in the descoped SP13.

Mission

The JSpOC uses JMS to enable the coordination, planning, synchronization, and execution of continuous, integrated space operations in response to tasking from the Commander, Joint Functional Component Command for Space (CDR JFCC SPACE), a component of U.S. Strategic Command, in support of national and Combatant Commander objectives. JSpOC will use JMS to provide the CDR JFCC SPACE with the ability to task sensors and process sensor data to monitor the space domain, predict, detect, and respond to space events, maintain, analyze, visualize, and disseminate SSA data, and collaborate with other forces.

Major Contractors

- Government prime contractor:
  - Air Force Space and Missile Systems Center – Los Angeles AFB, California
- System Integrator, Increments 1 and 2:
  - Space and Naval Warfare Systems Command – San Diego, California
- Increment 1 sub-contractors:
  - Intelligent Software Solutions, Inc. – Colorado Springs, Colorado
  - The Design Knowledge Company – Fairborn, Ohio
- Increment 2 sub-contractors:
  - Analytical Graphics Incorporated – Exton, Pennsylvania
  - Artificial Intelligence Solutions – Lanham, Maryland
  - Intelligent Software Solutions, Inc. – Colorado Springs, Colorado
  - The Design Knowledge Company – Fairborn, Ohio

Activity

- The Air Force has yet to conduct any OT&E for JMS Increment 2, but conducted significant development and developmental testing for JMS Increment 2, SP9 and 11 in 2016, including:
  - Three phases of functional developmental testing for SP9 between May and October 2016
  - Developmental cybersecurity assessment from February to March 2016 and testing of partial representations of JMS Increment 2 at the National Cyber Range as part of a continuum of cybersecurity assessment incorporated by the Program Office into the JMS development effort
- The Air Force Operational Test and Evaluation Center is planning an OUE of JMS Increment 2, SP9 following an IT&E period, and the developmental testing campaign, which is in progress.
- The Air Force completed a Critical Change review for JMS Increment 2 in August 2016, due to both schedule and cost increases. As a result of the review, the Air Force descoped JMS Increment 2, with a new final delivery date of May 2019 (originally July 2016). Descoped capabilities no longer being delivered with JMS Increment 2 include the majority of planned SP13 content, including a SAP-level enclave, automated high-priority tasking, advanced space order of battle tools, and the capability to ingest and process data from non-traditional SSA sensors.
- The Air Force is finalizing development of a revision to the JMS TEMP, to reflect program schedule and content changes, including the addition of OT&E for SP11, necessitated by the addition of functional capabilities.

Assessment

- As the Air Force has not conducted any OT&E for JMS Increment 2, there are no operational test data available.
- SP9 will require at least one more developmental testing phase than the three currently planned by the Air Force. The Program Office plans to reassess the SP9 and broader Increment 2 schedule at the completion of each developmental testing phase. DOT&E expects OT&E for SP9 to begin no earlier than June 2017.
- Delays in JMS Increment 2 capability delivery increase risk of late discovery of interoperability deficiencies between JMS and Space Fence Increment 1, and data processing capacity adequacy for JMS. Space Fence Increment 1 is currently in development, and a sub-scale Integration Test Bed representation of Space Fence is available for testing but is not connected nor prepared to connect to JMS. The deferral of Space Fence interoperability functionality to SP11 and the non-availability of JMS for interoperability testing between JMS and Space Fence will delay deficiency discovery and resolution for both JMS and Space Fence, and require the simulation of Space Fence-imposed workload in JMS testing, likely increasing cost and delivery schedule for both.
- The Air Force has deferred capability requirements from the validated JMS Capability Development Document, which were planned for delivery in SP13 and not included in SP11, to an undefined increment. The increment may overlap an as-yet-undefined program of record being planned to equip the new Joint Interagency Combined Space Operations Center (JICSPOC).

Recommendations

- Status of Previous Recommendations. The Air Force resolved one of the seven previous recommendations when it completed the planned technology refresh for Increment 1 equipment and continued acquisition, development, testing, and fielding of JMS Increment 2. The Air Force still needs to:
  1. Develop an acquisition strategy for delivery of capabilities post-Increment 2, including facilities and capabilities to support continuity of operations. This recommendation remains valid, given the restructure of Increment 2 and the nascent planning for a JICSPOC program of record.
  2. Investigate and resolve problems with external data source consistency, external interfaces, and support networks that will otherwise impede JMS end-to-end mission performance. The Air Force has made substantial progress in planning and assessing data source and external interface connectivity and interoperability, with the significant exception of JMS-Space Fence interoperability, as described above.
  3. Assess new Increment 2 capabilities and reassess JMS User Defined Operational Picture and net-centric capabilities to verify full JMS functionality. This is in progress and should be completed with SP11 OT&E.
  4. Develop and validate modeling and simulation tools to support evaluation of system capacity under high-user loading and evaluation of JMS high-accuracy catalog size and accuracy. This is in progress.
  5. Develop operationally-relevant measures to assess JMS system performance degradation due to cyber-attack. Provide capabilities to allow system administrators to monitor performance and take appropriate actions to mitigate operational impacts based on these measures. This recommendation remains valid and some progress has been made due to the Program Office's significant focus on cybersecurity assessment and hardening. Additional work remains to ensure JMS provides monitoring and insight sufficient to enable active cyber defense.
  6. Conduct independent, non-cooperative, threat representative penetration testing to assess protect, detect, react, and restore components of cybersecurity for Increment 2. This testing is planned for SP9 and SP11.
- FY16 Recommendation.
  1. The Air Force should commit resources to ensure interoperability testing between JMS and Space Fence Increment 1 in 2017, including dedicated schedule periods and use of partial- and full-hardware and software instances.

KC-46A

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted a second Operational Assessment (OA-2) from December 2014 through July 2016. The Air Force accomplished testing in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and the OA-2 test plan. DOT&E produced a KC-46A OA-2 report in August 2016.
- Initial air refueling (AR) testing in January and February 2016 uncovered unanticipated axial loads in the boom that approached the boom's structural limits, resulting in temporary suspension of further AR testing. Boeing redesigned the boom control system to address this problem and completed demonstration flights of the boom refueling system in July 2016.
- The KC-46A is trending to be an effective AR platform. It demonstrated a limited capability to refuel receiver aircraft (its primary mission) and to be refueled from tanker aircraft during OA-2. However, the demonstrations to date have been at a single point of the operational envelope for only five different receiver aircraft, during daylight only, and no aircraft have completed certification as a receiving platform. The AR boom receivers were the F-16, C-17, and A-10; the probe-drogue receivers were the F/A-18C and AV-8B.
- During OA-2 testing, the air refueling operators (AROs) identified a problem that can occur when the ARO station is set to "dual" operation such that the controls at both the primary and instructor station are active. When both positions apply a flight control stick command, the boom will move to a summed position due to the system's summation logic. There are situations where this could result in a rapid boom movement to the instructor-commanded position; if the receiver aircraft is in the path, the potential exists for the boom to inadvertently strike the receiver aircraft.
- The AROs also noted the long-wave infrared cameras produced an undesirable effect when interacting with the sun and clouds. For example, a solar trail occurs when the sun moves across the screen (such as during a turn) and leaves a persistent afterimage forming a line. Additionally, the ARO station screen overlays – which provide boom envelope position and other information – interfere with the ARO's ability to view and monitor AR operations.
- Testing during OA-2 did not identify any critical deficiencies with the cargo handling or aeromedical evacuation missions – though testing did identify deficiencies the Air Force should address.
- The KC-46A demonstrated satisfactory progress for operational suitability. The program is tracking better than planned on the reliability growth curve, as measured by Mean Time Between Inherent Failures. Several metrics are worse than thresholds, such as the aerial abort rate, cannot-duplicate rate for failures, Mean Time Between Unscheduled Maintenance, and break rate; however, these results are not surprising. The program is not planning to meet these requirements until 50,000 fleet flight hours, which will not occur until 2 to 3 years after Initial Operational Capability (IOC).

- During OA-2, testers discovered several cybersecurity vulnerabilities. The program plans to correct some of them prior to IOT&E. Corrections to others that are related to government-furnished equipment are under discussion.
- DOT&E evaluated the KC-46A survivability against kinetic and non-kinetic threats in four scenarios. Live fire test results, laboratory results, hardware-in-the-loop testing, and numerous vulnerability and susceptibility analyses provided source data for these evaluations. Results of these evaluations are in the classified annex to DOT&E's OA-2 report.
- DOT&E has previously assessed and continues to assess the KC-46A schedule as aggressive and unlikely to be executed as planned. At Milestone B, in February 2011, the Air Force had planned to be 66 percent complete by Milestone C. However, upon accomplishing Milestone C in August 2016, Boeing had completed only 30 percent of the total Engineering and Manufacturing Development (EMD) testing. Execution of the current schedule assumes historically unrealistic test aircraft fly and re-fly rates.

System

- The KC-46A aerial refueling aircraft is the first increment of replacement tankers (179) for the Air Force's fleet of more than 400 KC-135 tankers.
- The KC-46A design uses a modified Boeing 767-200ER commercial airframe with numerous military and technological upgrades, such as the fly-by-wire refueling boom, the remote AFO's station, 787 cockpit, additional fuel tanks in the body, and defensive systems.

- The KC-46A will provide both a boom and probe-drogue refueling capabilities. The KC-46A is equipped with an AR receptacle so that it can also receive fuel from other tankers, including legacy aircraft.
- The KC-46A is designed to have significant palletized cargo and aeromedical capacities; chemical, biological, radiological, and nuclear survivability; and the ability to host communications gateway payloads.
- Survivability enhancement features are incorporated into the KC-46A design.
  - Susceptibility is reduced with an Aircraft Survivability Equipment suite consisting of Large Aircraft Infrared Countermeasures (LAIRCM), a modified version of the ALR-69A Radar Warning Receiver (RWR), and a Tactical Situational Awareness System. The suite is intended to correlate threat information from pre-flight planning, the RWR, and other on- and off-board sources and to prompt the crew with an automatic re-routing suggestion in the event of an unexpected threat.
  - Vulnerability is reduced by adding a fuel tank inerting system and integral armor to provide some protection to the crew and critical systems.

Mission

Commanders will use units equipped with the KC-46A to perform AR to accomplish six primary missions to include nuclear operations support, global strike support, air bridge support, aircraft deployment, theater support, and special operations support. Secondary missions will include airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

Major Contractor

The Boeing Company, Commercial Aircraft in conjunction with Defense, Space & Security – Seattle, Washington

---

Activity

- The KC-46A program successfully accomplished a Defense Acquisition Board Milestone C decision in August 2016.
- DOT&E approved the Milestone C TEMP in November 2016, with concerns about adequate calendar time for correction of discrepancies or deficiencies between the end of developmental testing and the beginning of IOT&E.
- AFOTEC conducted OA-2 from December 2014 through July 2016. The Air Force accomplished testing in accordance with the DOT&E-approved TEMP and the OA-2 test plan. DOT&E produced a KC-46A OA-2 report in August 2016.
- Initial AR testing in January and February 2016 uncovered unanticipated axial loads in the boom that approached the boom's structural limits, resulting in temporary suspension of further AR testing. Boeing redesigned the boom control system to address this problem and completed demonstration flights of the boom refueling system in July 2016.
- Only Boeing and subcontractor laboratory testing on the Tactical Situational Awareness System and the modified ALR-69A RWR system has been completed to date; initial flight testing on these systems began in the spring of 2016, and will not be completed until shortly before IOT&E.
- LAIRCM testing provided hit point distribution data to inform the vulnerability assessment and to verify that LAIRCM performance on the KC-46A has not been degraded from previously demonstrated performance on other aircraft. Both system configurations (Block 20 with ultraviolet missile warning system and Block 30 with two-color infrared missile warning system) were included in the evaluation.
- Boeing and the Air Force still need to complete several tests that assess areas that significantly influence the aircraft's survivability. These include ground and flight testing of the On-Board Inert Gas Generation System, Electromagnetic Pulse (EMP) (delayed until April 2017), and thermal testing of the nuclear flash curtains.

Assessment

- DOT&E has assessed and continues to assess the KC-46A schedule as aggressive and unlikely to be executed as planned. At Milestone B, in February 2011, the Air Force had planned to be 66 percent complete by Milestone C. However, upon accomplishing Milestone C in August 2016, Boeing had completed only 30 percent of the total EMD testing. Many subsystems have only been tested in the laboratory. Execution of the current schedule assumes historically unrealistic test aircraft fly and re-fly rates.
- The KC-46A is trending to be an effective AR platform. It demonstrated a limited capability to refuel receiver aircraft (its primary mission) and to be refueled from tanker aircraft during OA-2. However, the demonstrations to date have been at a single point of the operational envelope for only five different receiver aircraft, during daylight only, and no aircraft have completed certification as a receiving platform. The AR boom receivers were the F-16, C-17, and A-10; the probe-drogue receivers were the F/A-18C and AV-8B.
- The current boom is a prototype designed to solve boom axial load problems encountered in early testing and is not production-representative. Wing refueling pods that meet all Federal Aviation Administration qualification requirements will not be available for two years.
- During OA-2 testing, the AROs identified a problem that can occur when the ARO station is set to "dual" operation such that the controls at both the primary and instructor station are active. When both positions apply a flight control stick command, the boom will move to a summed position

due to the system's summation logic. There are situations where this could result in a rapid boom movement to the instructor-commanded position; if the receiver aircraft is in the path, the potential exists for the boom to inadvertently strike the receiver aircraft. The Air Force and Boeing are working to resolve this deficiency.

- The AROs also noted the long-wave infrared cameras produced an undesirable effect when interacting with the sun and clouds. For example, a solar trail occurs when the sun moves across the screen (such as during a turn) and leaves a persistent afterimage forming a line. Additionally, the ARO station screen overlays – which provide boom envelope position and other information – interfere with the ARO's ability to view and monitor AR operations. The Air Force and Boeing are working to resolve this deficiency.
- Testing during OA-2 did not identify any critical deficiencies with the cargo handling or aeromedical evacuation missions – though testing did identify deficiencies the Air Force should address. Other secondary missions have not been tested.
- The KC-46A demonstrated satisfactory progress for operational suitability; however, it is premature to make definitive conclusions. The program is tracking better than planned on the reliability growth curve, as measured by Mean Time Between Inherent Failures. Several metrics are worse than thresholds, such as the aerial abort rate, cannot-duplicate rate for failures, Mean Time Between Unscheduled Maintenance, and break rate; however, these results are not surprising. The program is not planning to meet these requirements until 50,000 fleet flight hours, which will not occur until 2 to 3 years after IOC. Other metrics, including availability, mission-capable rate, sortie generation rate, and maintainability, cannot be estimated at this point in the program. Boeing owned, operated, maintained, and supplied the aircraft rather than the Air Force. Consequently, operational aircrew had minimal involvement in aircraft operations and there was no operational maintenance.
- DOT&E evaluated the KC-46A survivability against kinetic and non-kinetic threats in four scenarios. These threats include ballistic threats, light anti-aircraft artillery, man-portable air defense system missiles, radar-guided surface-to-air and air-to-air missiles, chemical and biological weapons, high power microwave, low power lasers, and EMP. Detailed results of these evaluations are in the classified annex to DOT&E's OA-2 report.
- The KC-46A EMP design margin was based on Military Standard (MIL-STD) 464 and the threat defined in MIL-STD 2169. After the fixed-price contract was awarded, the DOD instituted a new MIL STD 3023 that requires tanker aircraft supporting the nuclear deterrent mission to meet a 20-decibel (dB) EMP design margin versus the contractually required 6-dB EMP design margin. Unless additional tests are resourced, the Air Force or the U.S. Strategic Command will not know if the KC-46A meets the 20-dB EMP hardening requirement in MIL STD 3023.
- During OA-2, testers discovered several cybersecurity vulnerabilities. The program plans to correct some of them prior to IOT&E. Corrections to others that are related to government-furnished equipment are under discussion. Details are presented in the classified annex to the DOT&E OA-2 report.

Recommendations

- Status of Previous Recommendations. The Air Force has addressed all FY12 through FY14 recommendations. The Air Force still needs to address the following FY15 recommendations:
  1. Ensure all AR receiver aircraft are certified for use by operational aircrew early enough in IOT&E to permit sufficient operational testing.
  2. In conjunction with U.S. Strategic Command, determine whether its personnel can conduct the nuclear deterrence and strike missions with a KC-46A only having 6-dB EMP shielding as per the contract. If additional EMP shielding is deemed necessary, the Air Force should conduct testing as part of FOT&E to determine the actual KC-46A EMP design margin.
- FY16 Recommendations. The Air Force should:
  1. Develop an executable schedule that is based on historical fly and re-fly rates.
  2. Address the recommendations presented in the unclassified DOT&E KC-46A OA-2 report.
     - Verify boom loads are satisfactory under all operational conditions.
     - Address deficiencies with the ARO cameras, ARO station screen displays, and instructor control stick logic.
     - Address cybersecurity vulnerabilities.

Massive Ordnance Penetrator (MOP)

Executive Summary

- In March 2016, the Air Force successfully completed one weapon drop from the B-2 aircraft, and in June 2016, completed three weapon drops from two B-2 aircraft on a representative target. These tests, conducted at the White Sands Missile Range, New Mexico, demonstrated weapon effectiveness after the Air Force incorporated the Enhanced Threat Response (ETR) Phase 3 enhancements. ETR Phase 3 testing is complete and ETR Phase 4 testing will begin in FY17.
- DOT&E published a classified Early Fielding Report summarizing the ETR Phase 3 test results in September 2016.

System

- The GBU-57 Massive Ordnance Penetrator (MOP) is a large, GPS-guided, penetrating weapon with the ability to attack deeply-buried and hardened bunkers and tunnels. The warhead case is made from a special high-performance steel alloy and its design allows for a large explosive payload while maintaining the integrity of the penetrator case during impact.
- The B-2 Spirit is the only aircraft in the Air Force programmed to employ the MOP.
- The GBU-57 warhead is more powerful than its predecessors, the BLU-109 and GBU-28.
- The MOP is an Air Force-led, Quick Reaction Capability that is a SECDEF special interest effort and is under DOT&E oversight.

Mission

Combatant Commanders use the B-2 equipped with MOP to conduct pre-planned, day or night attacks against defended point targets vulnerable to blast and fragmentation effects and requiring significant penetration, such as hardened and deeply-buried facilities.

Major Contractor

The Boeing Company, Defense, Space & Security – St. Louis, Missouri

Activity

- In March 2016, the Air Force conducted one live weapon drop at the White Sands Missile Range, New Mexico, on a representative target to evaluate weapon functionality with the ETR-3 modifications. An Air Force B-2 aircraft flew the mission.
- In June 2016, the Air Force conducted a three-weapon test on a representative target. This testing was to evaluate weapon effectiveness. Two Air Force B-2 aircraft each flew one sortie to complete the mission.
- These events completed the ETR Phase 3 test.
- DOT&E submitted a classified Early Fielding Report in September 2016 detailing the results of ETR Phase 3.

Assessment

- The ETR Phase 3 testing was successful in demonstrating weapon effectiveness with the current weapon configuration.
- Nonetheless, significant differences between pre-test modeling predictions and actual test results indicate the need for provision of additional modeling capacity, such as that available using the Department's High-Performance Computing facilities.
- The Air Force will continue with ETR Phase 4 testing in FY17.

Recommendations

- Status of Previous Recommendations. There were no previous recommendations for this program.
- FY16 Recommendations. None.

Miniature Air Launched Decoy (MALD) and Miniature Air Launched Decoy – Jammer (MALD-J)

Executive Summary

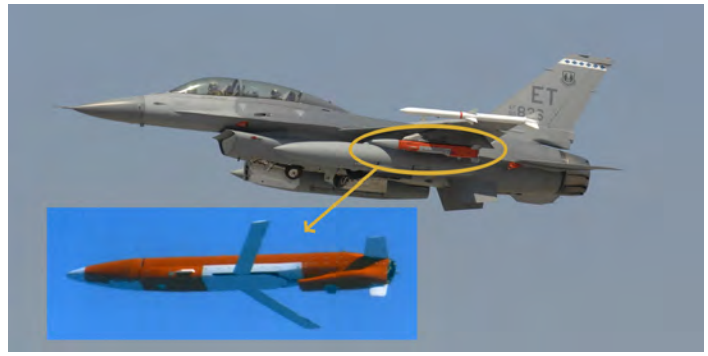
- The Miniature Air Launched Decoy – Jammer (MALD-J) mission planning tools, with the latest software upgrades, can support the 72-hour Air Tasking Order (ATO) planning cycle.
- Flight testing of a navigational system upgrade was stopped because of an anomaly observed in June 2016. The Program Office has corrected the software errors and verified the correction in both ground and flight testing in August 2016 and September 2016, respectively.

System

- MALD is a small, low-cost, expendable, air-launched vehicle that replicates how fighter, attack, and bomber aircraft appear to enemy radar operators.
- MALD-J is an airborne close-in jammer for electronic attack with the ability to loiter on station.
- MALD-J will jam specific Early Warning/Ground Control Intercept/Acquisition radars while retaining the capabilities of the MALD.
- MALD-J will stimulate and degrade an enemy's integrated air defense system.
- The F-16 C/D and B-52H are the lead aircraft to employ MALD and MALD-J.

Mission

- Combatant Commanders will employ units equipped with MALD or MALD-J to improve battlespace access for airborne strike forces by deceiving, distracting, or saturating enemy radar operators and integrated air defense systems.



  - MALD is designed to allow an airborne strike force to accomplish its mission by deceiving enemy radars and air defense systems to treat MALD as a viable target.
  - MALD-J is designed to allow an airborne strike force to accomplish its mission by jamming specific enemy radars and air defense systems to degrade or deny detection of friendly aircraft or munitions.
  - MALD J-equipped forces will be able to stimulate an enemy's integrated air defense system enabling friendly forces to target and engage enemy components.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- In January 2016, the Air Force Operational Test and Evaluation Center (AFOTEC) completed ground testing of the GPS Aided Inertial Navigation System (GAINS) obsolescence upgrade (known as GAINS2) to the MALD-J at the National Radar Cross Section Test Facility, New Mexico, which included a side-by-side test between a GAINS unit and a GAINS2 unit.
- In June 2016, the 28th Test and Evaluation Squadron (TES) partially executed a Force Development Evaluation (FDE) at White Sands Missile Range, New Mexico, in conjunction with a MALD-J Reliability Assessment Program mission, to assess the performance of the GAINS2 obsolescence upgrade to the MALD-J. The 28th TES launched only two missiles: one in an uncontested environment and one in a GPS-contested environment.
- In July 2016, the Program Office and Raytheon Missile Systems completed a review for the navigation anomaly observed in a GPS-contested environment during the FDE in June 2016.
- From March through June 2016, the Program Office completed four data collection events with respect to mission planning for MALD-J on the F-16 and B-52 platforms; one at Barksdale AFB in Louisiana, one at Eglin AFB in Florida, one at Spangdahlem AFB in Germany, and one at Aviano AFB in Italy.
- The Program Office verified during ground testing in August 2016, and during flight testing in September 2016, that the software update corrected the software anomaly.

Assessment

- MALD-J (and MALD) testing was done in accordance with a DOT&E approved test plan.
- The latest mission planning data collections for the MALD-J program show marked reduction in the time needed to plan a full load of MALD-J vehicles. The mission planning tools, with the latest software upgrades, can support the 72-hour ATO planning cycle.
- Preliminary results from ground testing indicate improved performance of the GAINS2 system in a GPS-contested environment as compared to the GAINS.
- Due to a navigation anomaly observed during the FDE in June 2016, no assessment of the GAINS2 free flight performance in a GPS contested environment can be made.
- The Program Office concluded that the MALD-J failed to reacquire any GPS satellites when the navigation system exited the GPS contested environment because of software errors introduced by Raytheon Missile Systems.

Recommendations

- Status of Previous Recommendations. The Air Force satisfactorily addressed the one remaining FY14 recommendation and one of the three FY15 recommendations. The Air Force still should:
  1. Incorporate additional operational elements into the mission-level simulation in the Digital Integrated Air Defense System.
  2. Improve horizontal navigational accuracy of the MALD-J (and MALD) vehicle.
- FY16 Recommendation.
  1. Once the GAINS2 software corrections are verified, the Air Force should return to free flight testing of the GAINS2 in a GPS-contested environment.

MQ-9 Reaper Armed Unmanned Aircraft System (UAS)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) completed FOT&E of the MQ-9 Block 5 Remotely Piloted Aircraft (RPA), Block 30 Ground Control Station (GCS), and Operational Flight Program (OFP) 904.6 software suite revision K in accordance with the DOT&E-approved test plan. The results from the FOT&E demonstrated the following:
  - The MQ-9 Unmanned Aircraft System (UAS) configuration tested is not operationally effective and not operationally suitable. The system was unable to conduct the all-weather hunter mission role operations using onboard systems.
  - The MQ-9 UAS evaluated in the FOT&E is not capable of conducting wide-area searches to hunt fixed or moving targets with the Lynx Synthetic Aperture Radar (SAR) system. The MQ-9 Lynx SAR does not provide a useful operation for the Block 5 RPA/Block 30 GCS due to unstable and unmanageable aircraft and GCS software configuration problems; human machine interface complexity; inadequate and incomplete technical orders; and persistent in-flight radar mode failures.
  - The Block 5 RPA/Block 30 GCS MQ-9 UAS retains the legacy MQ-9 capability to conduct cued area searches for fixed and moving targets with the Multi-spectral Targeting System (MTS) B electro-optical/infrared sensor, and to employ legacy AGM-114 HELLFIRE II missiles and GBU 12 laser guided bombs. Additionally, the FOT&E results demonstrated the MQ-9 UAS can effectively employ GBU-38 JDAM bombs against stationary targets, as long as target coordinates are provided by off-board sources.
  - The Block 5 RPA and Block 30 GCS are not operationally suitable. Testing showed these systems experience high abort rates and break often.
- The MQ-9 Block 5 RPA is subject to overheating problems in operationally relevant environments.
  - Block 5 RPA subsystems may overheat in hot weather prior to take-off, leading to mission aborts. The installation of an aircraft cooling plenum and addition of a new, more powerful ground-cooling cart in FY15 mitigates some of the RPA avionics bay overheating problems identified in FY14. However, these measures do not eliminate all overheating problems in hot weather operating environments.
  - Inherent Block 5 RPA design limitations lead to thermal management problems that were not fully resolved by the aircraft cooling plenum or the new ground-cooling cart. As highlighted in the DOT&E FY15 Annual Report, although these measures mitigated RPA forward avionics bay redundant control module and transmitter overheating shortfalls, power and thermal management problems that can preclude charging batteries on the ground can lead to depleted batteries prior to take-off and may force mission aborts.
- In FY15, the Air Force adopted a hybrid acquisition strategy for the MQ-9 program of record. The Air Force intended for the acquisition strategy to provide a series of bundled MQ-9 software/hardware releases under an accelerated development and testing schedule. The first release of planned capabilities under this construct envisioned for FY17 delivery is expected to deliver in FY18.
- The final configuration of the MQ-9 Increment One UAS continued to evolve. As of the end of FY16, the Air Force indicated it plans to incorporate an improved MTS-B electro-optical/infrared sensor, additional weapons, new avionics hardware, and further system software revisions into the existing program of record.
- General Atomics delivered the last of 195 Block 1 RPAs to the Air Force in 2QFY15, and then transitioned the production line to Block 5 RPAs. As of 3QFY16, General Atomics had delivered 12 of 155 planned Block 5 RPAs. Total Air Force MQ-9 deliveries as of 3QFY16 include 207 of 350 planned MQ-9s (Block 1 and Block 5 combined). General Atomics plans to deliver the final Block 5 RPA in FY21.
- The Air Force plans to field the Block 5 RPA and Block 30 GCS in 1QFY17, and will complete delivery of the MQ-9 program of record fleet under low-rate initial production.

System

- The MQ-9 Reaper UAS is a remotely piloted and armed aircraft system that uses optical, infrared, and radar sensors to locate, identify, target, and attack ground targets.
  - The MQ-9 RPA is a medium-sized aircraft that has an operating ceiling up to 50,000 feet, an internal sensor payload of 800 pounds, an external payload

of 3,000 pounds, and an endurance of approximately 12 hours.
  - Aircraft sensors include the MTS-B electro-optical and infrared targeting sensor and the Lynx SAR system.
  - The GCS commands the MQ-9 RPA for launch, recovery, and mission control of sensors and weapons. RPA launch and recovery operations use C band line-of-sight datalinks, and RPA mission control uses Ku band satellite links.
- The fielded Block 1 MQ-9 RPA carries AGM-114 HELLFIRE II anti-armor precision laser-guided missiles, and GBU-12 500-pound, laser-guided bombs.
- The Air Force is using an evolutionary acquisition approach for meeting Increment One Capability Production Document requirements, with Block 1 and Block 5 RPAs and Block 15 and Block 30 GCSs.
- The Air Force is currently fielding the Block 1 RPA and the Block 15 GCS and will field the Block 5 RPA and Block 30 GCS in 1QFY17.
- The Air Force designed the Block 5 RPA to incorporate improved main landing gear, an upgraded electrical system with more power, an additional ARC-210 radio, encrypted datalinks, a redesigned avionics bay and digital electronic engine control system, the BRU-71 bomb rack, high-definition video, and upgraded software to allow the two-person aircrew to operate all onboard sensors and systems.
- The Air Force designed the Block 30 GCS to incorporate upgraded flight control displays and avionics, secure digital datalinks, Integrated Sensor Control System, Continuous Look Attack Management for Predator, Control of Lynx and Analysis Workstation software, and high-definition multi-function displays.

Mission
- Combatant Commanders use units equipped with the MQ-9 to conduct armed reconnaissance and pre-planned strikes. When provided wide-area search cues from off-board sources, units equipped with MQ-9s can execute cued searches to find, fix, track, target, engage, and assess critical emerging targets (both moving and stationary).
- MQ-9 units can also conduct aerial intelligence gathering, reconnaissance, surveillance, and target acquisition for other airborne platforms.

Major Contractor
General Atomics Aeronautical Systems Inc. – San Diego, California

---

Activity
- The Air Force conducted MQ-9 testing in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- AFOTEC completed FOT&E of the Block 5 RPA, Block 30 GCS, and OFP 904.6 in 4QFY16 in support of Air Force 1QFY17 planned operational fielding. Testing evaluated the MQ-9 all-weather, wide-area search capability across multiple operational mission sets to determine the system's ability to hunt and kill fixed and moving targets using system capabilities and weapons. Additional testing included a cybersecurity Adversarial Assessment and hot and cold weather tests.
  - During the FOT&E, AFOTEC discovered a deficiency in the ability of the MTS-B to track targets without breaking lock, and declared a test pause. During the pause, the Air Force determined the root cause of the deficiency was due to a software anomaly. The Air Force corrected the problem and evaluated the fix in subsequent developmental regression testing. Upon software fix incorporation, AFOTEC resumed the FOT&E and re-accomplished the MTS-B-related FOT&E test points.
  - AFOTEC terminated MQ-9 Lynx SAR FOT&E testing without completing the scope of planned Lynx SAR test events. Persistent GCS configuration problems, incomplete technical orders, and software complexities precluded contract maintainers from effectively configuring and troubleshooting, and precluded aircrews from effectively employing the system.
- In conjunction with the FY16 FOT&E, AFOTEC and the 57th Information Aggressor Squadron conducted a cybersecurity Adversarial Assessment of the MQ-9 Block 5 RPA/Block 30 GCS.
- In FY15, the Air Force adopted a hybrid acquisition strategy for the MQ-9 program of record. The Air Force intended for the acquisition strategy to provide a series of bundled MQ-9 software/hardware releases under an accelerated development and testing schedule. The first release of planned capabilities under this construct is expected to deliver in FY18.
- The final configuration of the MQ-9 Increment One UAS continued to evolve. As of the end of FY16, the Air Force indicated it plans to incorporate an improved MTS-B electro-optical/infrared sensor, additional weapons, new avionics hardware, and further system software revisions into the existing program of record.
- General Atomics delivered the last of 195 Block 1 RPAs to the Air Force in 2QFY15, and then transitioned the production line to Block 5 RPAs. As of 3QFY16, General Atomics had delivered 12 of 155 planned Block 5 RPAs. Total Air Force MQ-9 deliveries as of 3QFY16 include 207 of 350 planned MQ-9s (Block 1 and Block 5 combined). General Atomics plans to deliver the final Block 5 RPA in FY21.
- The Air Force plans to field the Block 5 RPA and Block 30 GCS in 1QFY17, and will complete delivery of the MQ-9 program of record fleet under low-rate initial production.

Assessment

- The FY16 MQ-9 FOT&E was intended to evaluate deferred Increment One system and operational mission capabilities not evaluated during the 2007 IOT&E. During IOT&E, the MQ-9 Lynx SAR system integration was immature, and the MQ-9 hunter mission role was not evaluated due to this shortfall. The Air Force intended to satisfy the hunter mission role through the acquisition of the Block 5 RPA and Block 30 GCS, and this configuration entered production in 2011. However, the MQ-9 Block 5 RPA as tested in the FY16 FOT&E and that will field to operational units in FY17 cannot conduct an all-weather hunter mission role using the Lynx SAR system.
  - FOT&E results demonstrated the MQ-9 Increment One UAS is not operationally capable of conducting wide-area searches to hunt fixed or moving targets with the Lynx SAR radar. The MQ-9 UAS is not operationally effective in this mission role.
  - Operational aircrews were not able to successfully conduct radar search and targeting tasks due to Lynx SAR radar instability, persistent aircraft and GCS software configuration problems, human machine interface complexity, inadequate and incomplete technical orders, and in-flight radar mode failures.
  - Deficient technical order publications further precluded aircrews and contractor maintainers from troubleshooting radar problems when they occurred during FOT&E missions.
  - Aircrews could not reliably execute legacy radar tasks that had been successfully demonstrated in 2013 Block 1 RPA operational testing (SAR spot imaging to support target location determination and ground moving target indicator detection and cueing) with the Block 5 RPA/Block 30 GCS system. As described above, software complexity, technical order deficiencies, and maintainer inability to troubleshoot radar problems precluded mission accomplishment using the radar system.
  - Based on the shortfalls realized in FOT&E, the MQ-9 Lynx SAR as tested does not provide an operationally useful capability to search for targets for the Block 5 RPA and Block 30 GCS UAS configuration.
- The MQ-9 Block 5 RPA demonstrated adequate MTS-B cued-search, track, and laser-guided weapons support capabilities during operational mission tasks executed in the course of FY16 FOT&E.
- The FY16 FOT&E confirmed the Block 5 RPA/Block 30 GCS system can successfully employ GBU-38 JDAM bombs (when target coordinates are provided by off-board sources), and can employ legacy AGM 114 HELLFIRE II laser-guided missiles and GBU 12 laser-guided bombs.
- FOT&E results established that the Block 5 RPA and Block 30 GCS are not operationally suitable. Testing showed this system breaks more often and is harder to maintain than the legacy Block 1 RPA and Block 15 GCS.
- The MQ-9 Block 5 RPA is subject to overheating problems in operationally relevant environments.
  - Block 5 RPA subsystems may overheat in hot weather prior to take-off, leading to mission aborts. The installation of an aircraft cooling plenum and addition of a new, more powerful ground-cooling cart in FY15 mitigates some of the RPA avionics bay overheating problems identified in FY14. However, it does not eliminate all overheating problems in hot weather operating environments.
  - Inherent Block 5 RPA design limitations led to thermal management problems that are not fully resolved by the installed aircraft cooling plenum or the new ground-cooling cart. As highlighted in the DOT&E FY15 Annual Report, although these measures mitigated RPA forward avionics bay redundant control module and transmitter overheating shortfalls, power and thermal management problems that can preclude charging batteries on the ground can lead to depleted batteries prior to take-off and forcing mission aborts.
- Aircrew Block 5 RPA and Block 30 GCS technical orders do not support proper system operations. Some areas of the technical orders are too long and complex (e.g., preflight checklists). Other areas lack proper instructions for accomplishing mission tasks (e.g., Lynx SAR operations) and problem resolution (e.g., fuel tank overheating cautions).
  - Contractor personnel maintained the Block 30 GCS during FOT&E. The Air Force plans to field the Block 30 GCS in 1QFY17 and maintain the system with only Air Force personnel. It is likely that Air Force personnel will encounter the same maintenance challenges that contractor maintenance personnel experienced during testing.
- The Air Force originally intended to fulfill the MQ-9 Increment One requirements with a final UAS configuration consisting of the Block 5 RPA, Block 30 GCS, and OFP 904.6. The Air Force currently plans to complete the MQ-9 Increment One system with a Block 50 GCS and a future system OFP. The Air Force delayed Block 50 GCS development, and initial production of Block 50 GCS units will not occur until FY19. Subsequent AFOTEC FOT&E of the Block 50 GCS and the system capabilities being developed under the Air Force hybrid acquisition strategy may not occur until FY21. A new TEMP will be required to document the incorporation of new program of record content, and the test strategy and resources necessary to develop and evaluate the Block 50 GCS and associated MQ-9 capabilities.

Recommendations

- Status of Previous Recommendations. In FY16, the Air Force completed the FOT&E. The Air Force made progress toward but did not satisfy the FY15 recommendations to resolve the hot weather operating shortfalls.
- FY16 Recommendations. The Air Force should:
  1. Correct the Block 5 RPA/Block 30 GCS Lynx SAR shortfalls identified during FY16 FOT&E. Once the radar problems are resolved, re-accomplish formal FOT&E to confirm the MQ-9 UAS ability to conduct wide-area search

tasks to hunt moving and fixed targets in a hunter mission role, and to demonstrate the ability to generate own-ship precision coordinates necessary for JDAM employment.

2. Resolve the remaining Block 5 RPA power and thermal management operating shortfalls to meet Air Force operating environment requirements.
3. Correct MQ-9 operator and maintainer technical orders deficiencies to enable effective system operation and maintenance.
4. Develop and submit a new TEMP for DOT&E approval, documenting the incorporation of new program of record content (e.g., the Block 50 GCS) and the T&E strategy and resources required to mature and test these capabilities and systems.

QF-16 Full-Scale Aerial Target (FSAT)

Executive Summary

- The Air Force completed QF-16 radar cross section (RCS) measurements in FY16.
- The Air Force has not accomplished cybersecurity testing in accordance with the DOT&E IOT&E recommendation and cybersecurity policy memorandum, dated August 1, 2014.
- The Air Force should continue, as it did in FY16 and FY17, to provide procurement funding for at least 25 Full-Scale Aerial Targets (FSATs) per year to meet Service-coordinated aerial target requirements, in compliance with Resource Management Decision 700.
- The Air Force should support the OSD-sponsored study to address shortfalls in testing against fifth-generation airborne threats, and be prepared to fund and implement the recommendations that are assigned for Air Force execution.

System

- The QF-16 is the latest FSAT designed to test and evaluate U.S. weapon systems and assist in developing tactics, techniques, and procedures to counter fighter-size airborne threats. The DOD is replacing the current FSAT, the QF-4, due to its increasing dissimilarity from current and projected air-superiority threats, declining supportability, and depletion of suitable F-4 airframes.
- The QF-16 system is composed of regenerated F-16 Block 15, 25, and 30 aircraft equipped with Drone-Peculiar Equipment to enable remote command and control, missile trajectory scoring, and safe flight termination. Like the QF-4, the QF-16 is capable of manned and Not Under Live Local Operator flight operations. It will operate from Tyndall AFB, Florida, using the Gulf Range Drone Control System, and Holloman AFB, New Mexico, using the White Sands Integrated Target System located at White Sands Missile Range, New Mexico.
- The QF-16 retains F-16 flight performance characteristics and payload capabilities including supersonic, after-burning engine, high-G maneuvering, complex electronic attack, and expendable countermeasures.

Mission

The DOD uses FSATs to:

- Provide threat-representative presentations for developmental and operational test and evaluation for U.S. weapon systems, as mandated by section 2366, title 10 U.S. Code.
- Continuously evaluate fielded air-to-air missile capabilities while providing live missile training for combat air crews through Air Force and Navy Weapon Systems Evaluation Programs.

Major Contractor

The Boeing Company – St. Louis, Missouri

Activity

- The Air Force completed RCS measurements in FY16 and demonstrated that the QF-16 meets the Capability Development Document requirements.
- The Air Force Life Cycle Management Center, with the support of the Air Force Operational Test and Evaluation Center, is in the process of test planning to comply with DOT&E cybersecurity testing requirements.

Assessment

- The QF-16 program currently lacks Air Force funding to complete additional cybersecurity testing. Using current program funding, the Air Force Life Cycle Management Center awarded a contract to Boeing to continue cybersecurity test planning in accordance with DOT&E guidance.
- The Air Force did not require QF-16 to represent fifth generation airborne threat systems (including radio frequency low-observability characteristics, internally-carried advanced electronic attack, and low probability of intercept sensors). DOT&E continues to emphasize that existing aerial targets, including the QF-16, are insufficient for adequate operational testing of U.S. weapon systems. Air Force RCS measurements show that QF-16 can only partially satisfy the test requirements for fifth generation full-scale targets.
  - In the Air Superiority Target Phase I Analysis of Alternatives Final Report (March 15, 2007), the Air Force recommended further study to produce user consensus on critical characteristics of future aerial targets and

to determine capabilities and shortfalls in existing test resources.
- Multiple stakeholders within Congress, OSD, the Air Force, and the Navy, support the requirement for a fifth generation FSAT. OSD is leading a study to assess both short- and long-term fifth generation FSAT options, with a scheduled completion of March 2017.

- Vector Scoring System (VSS) reliability was noted as a problem in the 2015 QF-16 IOT&E report. The Air Force continues to monitor VSS reliability. The VSS hardware changes made for production aircraft, along with checkout and maintenance procedure updates, have shown improvement in VSS reliability. Additional data collection is ongoing to fully assess if the system will support compliance with the QF-16's Mean Time Between Failure requirement.
- In late June 2015, Boeing performed sample inspections on a QF-16 at Cecil Field, Florida, and discovered workmanship deficiencies with wire splices, termination, and routing. As a result of these findings, they broadened the inspection population to the first three production aircraft already delivered to Tyndall AFB, Florida, and found similar problems. Corrective actions were completed and the Program Office received clearance in FY16 to provide full QF-16 services. Air Combat Command declared QF-16 Initial Operational Capability at Tyndall AFB, Florida, in September 2016, with a total of 15 QF-16s available for target operations.

Recommendations
- Status of Previous Recommendations. The Air Force completed RCS measurements in FY16 and has continued to monitor and improve VSS reliability. The Air Force still needs to address the recommendations to accomplish cybersecurity testing in accordance with the DOT&E cybersecurity policy memorandum, dated August 1, 2014.
- FY16 Recommendations. The Air Force should:
  1. Support the OSD-sponsored study to address shortfalls in testing against fifth-generation airborne threats, and be prepared to fund and implement the recommendations that are assigned for Air Force execution.
  2. Continue to monitor VSS reliability to ensure the corrections that were implemented in production aircraft will support compliance with the QF-16's Mean Time Between Failure requirement.

RQ-4B Global Hawk High-Altitude Long-Endurance Unmanned Aerial System (UAS)

Executive Summary

- The RQ-4B Block 40/Multi-Platform Radar Technology Insertion Program (MP-RTIP) IOT&E began in September 2015 and completed in January 2016. DOT&E assessed that the system demonstrated the capability to provide exploitable synthetic aperture radar (SAR) and Ground Moving Target Indicator (GMTI) data. The system met joint interoperability requirements. A cybersecurity Adversarial Assessment conducted in conjunction with the IOT&E identified vulnerabilities that are documented in the classified DOT&E IOT&E report. The RQ-4B Global Hawk Block 40 is operationally suitable and can generate and sustain the long-endurance missions necessary to support non-continuous operations representative of the current combat tempo. The RQ-4B Global Hawk Block 40 suitability has significantly improved over both the 2013 RQ-4B Block 40 Operational Utility Evaluation (OUE) and 2010 RQ-4B Block 30 IOT&E results. MP-RTIP sensor stability has also significantly improved since the RQ-4B Block 40 OUE.
- DOT&E approved the Air Force Capstone Test and Evaluation Master Plan (TEMP) in June 2016, which provides an overarching test approach for the system architecture and capability upgrades included in the new program baseline and future modernization programs. DOT&E anticipates the program will develop TEMP annexes according to the requirements and schedule documented in the approved Capstone TEMP.
- The Air Force is currently planning to conduct RQ-4B Block 30/Airborne Signals Intelligence Payload (ASIP) FOT&E in conjunction with the initial phases of the RQ-4B modernization program in FY18. This test will include a re-evaluation of the RQ-4B Block 30 Signals Intelligence (SIGINT) mission capabilities with the ASIP sensor as well as an assessment of previously identified ground station, air vehicle, communication system, interoperability, and cybersecurity shortfalls.

System

- The RQ-4B Global Hawk is a remotely-piloted, high-altitude, long-endurance airborne intelligence, surveillance, and reconnaissance (ISR) system that includes the Global Hawk unmanned air vehicle, various intelligence and communications relay mission payloads, and supporting command and control ground stations.
- The RQ-4B Global Hawk Block 30 system is equipped with a multi-intelligence payload that includes both the Enhanced Integrated Sensor Suite imagery intelligence payload and ASIP SIGINT sensor.
- The RQ-4B Block 40 system is equipped with the MP-RTIP synthetic aperture radar payload designed to simultaneously collect imagery intelligence on stationary ground targets and track ground-moving targets.
- All RQ-4B systems use line-of-sight and beyond line-of-sight communication systems to provide air vehicle command and control and transfer collected intelligence data to grounds stations for exploitation and dissemination.
- The Air Force Distributed Common Ground System (AF DCGS) supports ISR collection, processing, exploitation, analysis, and dissemination for both Block 30 and 40 RQ-4B Global Hawk systems. The AF DCGS employs global communications architecture to connect multiple intelligence platforms and sensors to numerous Distributed Ground Stations where intelligence analysts produce and disseminate intelligence products.

Mission

- Commanders use RQ-4 Global Hawk reconnaissance units to provide high-altitude, long-endurance intelligence collection capabilities to support theater operations. Units equipped with RQ-4B Global Hawk use line-of-sight and beyond line-of-sight satellite datalinks to control the Global Hawk system and transmit collected intelligence data.
- Operators collect imagery and SIGINT data to support ground units and to identify intelligence-essential elements of information for theater commanders.
- Ground-based intelligence analysts exploit collected imagery, ground-moving target, and SIGINT to provide intelligence products that support theater operations.
- Forward-based personnel can receive imagery intelligence directly from Global Hawk.

Major Contractor
Northrop Grumman Aerospace Systems, Strike and Surveillance Systems Division – San Diego, California

Activity

- As of September 2016, the Air Force has taken delivery of 18 of 21 RQ-4B Block 30 air vehicles and all 11 RQ-4B Block 40 air vehicles, along with 9 Mission Control and 10 Launch and Recovery ground stations.
- The Air Force is currently planning to conduct FOT&E in conjunction with the initial phases of the RQ-4B modernization program in FY18. This test will include a complete re-evaluation of the RQ-4B Block 30 SIGINT mission capabilities with the ASIP sensor as well as an assessment of previously identified ground station, air vehicle, communication system, interoperability, and cybersecurity shortfalls.
- DOT&E approved the Air Force Capstone TEMP in June 2016, which provides an overarching test approach for the system architecture and capability upgrades included in the new program baseline and future modernization programs. DOT&E anticipates the program will develop TEMP annexes according to the requirements and schedule documented in the approved Capstone TEMP.
- The Air Force did not conduct any RQ-4B Block 30 operational testing in FY15. The Air Force continued to sustain operations for 18 Block 30 aircraft at Beale AFB, California, and at forward operating bases in U.S. Pacific Command, U.S. Central Command, and U.S. European Command operating areas.
- The Air Force is currently developing a comprehensive program test strategy and TEMP to correct previously identified RQ-4B Block 30 capability shortfalls and test a series of modernization upgrades. This strategy will identify the next collection of significant RQ-4B Block 30 FOT&E events planned for FY18. Events include re-evaluation of previously identified ASIP/SIGINT mission capability shortfalls, interoperability deficiencies, MS-177 sensor integration, weather radar integration, mission planning upgrades, and other system modernization changes.
- The RQ-4B Block 40/MP-RTIP IOT&E began in September 2015 and completed in December 2015. The Air Force conducted testing in accordance with the DOT&E-approved test plan. DOT&E approved the Block 40 IOT&E test plan in May 2015.

Assessment

- In July 2016, DOT&E published the classified RQ-4B Global Hawk Block 40 IOT&E report based on test results from the RQ-4B Block 40/MP-RTIP IOT&E conducted from September 2015 through January 2016.
  - The system demonstrated the capability to provide exploitable SAR and GMTI data. Both SAR and GMTI data met most operational requirements and provided actionable intelligence products to operational users. However, inadequate training, procedures, tools, communication, and management hindered the ability of the AF DCGS to exploit GMTI data in near real-time.
  - The system met joint interoperability requirements.
  - A cybersecurity Adversarial Assessment conducted in conjunction with the IOT&E identified vulnerabilities that are documented in the classified IOT&E report.
  - The RQ-4B Global Hawk Block 40 is operationally suitable and can generate and sustain the long-endurance missions necessary to support non-continuous operations representative of the current combat tempo. The RQ-4B Global Hawk Block 40 suitability has significantly improved over both the 2013 RQ-4B Block 40 OUE and 2010 RQ-4B Block 30 IOT&E results. However, the Air Force continues to operate the RQ-4B Global Hawk Block 40 at a rate of three missions per week based on the suitability results from the 2010 RQ-4B Block 30 IOT&E. Despite initial expectations (requirements) that called for a single Global Hawk orbit to provide near-continuous on-station coverage for 30 days, the Air Force has since adopted a combat tempo of 3 long duration (approximately 28 hours) sorties a week over 30 days or more.
  - MP-RTIP sensor stability has also significantly improved since the RQ-4B Block 40 OUE.

Recommendations

- Status of Previous Recommendations. The Air Force made progress toward addressing FY15 recommendations. The Air Force completed an RQ-4B Capstone TEMP to guide developmental and operational testing of these systems. The Air Force has not completed a plan to complete the FOT&E for the RQ-4B Block 30 SIGINT mission using the ASIP sensor.
- FY16 Recommendations. The Air Force should:
  1. Develop RQ-4B program Capstone TEMP annexes to guide execution of the RQ-4B Global Hawk Block 30 FOT&E and to define operational test requirements for future Block 30 and Block 40 system upgrades.
  2. Develop a plan to complete the FOT&E for the RQ-4B Block 30 SIGINT mission using the ASIP sensor.
  3. Develop a comprehensive plan to address cybersecurity deficiencies observed during RQ-4B Global Hawk Block 40/MP-RTIP IOT&E.
  4. Develop AF DCGS training, procedures, tools, communication, and management enhancements to allow exploitation of RQ-4B Global Hawk Block 40 GMTI data in near real-time.

Small Diameter Bomb (SDB) II

Executive Summary

- The Small Diameter Bomb (SDB) II developmental testing is ongoing. Government Confidence Testing (GCT) began in October 2016. The Air Force awarded the Low-Rate Initial Production Lot 2 contract for 250 weapons in September 2016.
- SDB II is progressing towards meeting its effectiveness, reliability, and lethality requirements in the Normal Attack (NA) mode, which is the primary employment method for SDB II. The Air Force also successfully demonstrated Laser Illuminated Attack (LIA) and Coordinate Attack (CA) in 2016.
- The program has implemented corrective actions and fixes for all failure modes discovered in test. The weapon failed one environmental test related to the shipboard environment. The program implemented corrective action and successfully qualified design changes in corrosion, temperature, altitude and humidity, and vibration environments.
- IOT&E is scheduled to begin 4QFY17 with an adequately resourced test program.

System

- The SDB II is a 250-pound, air-launched, precision-glide weapon that uses deployable wings to achieve stand-off range. F-15E aircraft employ SDB IIs from the BRU-61/A four weapon carriage assembly.
- SDB II is designed to provide the capabilities deferred from SDB I. It includes a weapon datalink allowing for post-launch tracking and control of the weapon, as well as a tri-mode seeker to provide the ability to strike mobile targets in all weather.
- SDB II combines Millimeter-Wave radar, imaging infrared, and laser-guidance sensors in a terminal seeker, in addition to a GPS and an Inertial Navigation System to achieve precise guidance accuracy in adverse weather.
- The SDB II incorporates a multi-function warhead (blast, fragmentation, and shaped charge jet) designed to defeat armored and non-armored targets. The weapon can be set to initiate on impact, at a preset height above the intended target, or in a delayed mode.

- SDB II provides increased weapons load per aircraft compared to legacy air-to-ground munitions used against offensive counter-air, strategic attack, interdiction, and close air support targets in adverse weather.
- SDB II is intended to provide reduced collateral damage while achieving kills across a broad range of target sets by precise accuracy, small warhead design, and focused warhead effects.
- There are three principal attack modes: NA, LIA, and CA. SDB II can be used against moving or stationary targets using its NA (radar/ infrared sensors) or LIA modes, and fixed targets with its CA mode.

Mission

- Combatant Commanders will use units equipped with SDB II to attack stationary and moving ground targets in degraded weather conditions at stand-off ranges.
- An SDB II-equipped unit or Joint Terminal Attack Controller will engage targets in dynamic situations and use a weapon datalink network to provide in-flight target updates, in-flight retargeting, weapon in-flight tracking, and, if required, weapon abort.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- As of 2016, the Air Force has successfully completed 16 NA Guided Test Vehicle (GTV) and 10 Live Fire (LF) developmental tests against moving and stationary targets. Four GTV and 6 LF tests were conducted with Ultra High Frequency updates; 12 GTV and 4 LF test shots were conducted with Link 16 updates. NA is the primary employment method for SDB II. Also, in 2016, the Air Force completed three CA and four LIA GTV tests.
- The Program Office completed 15 rounds of seeker Captive Flight Tests, resulting in over 2,260 target runs in a wide variety of terrain and environmental conditions. These tests provided terabytes of seeker performance data and logged over 483 hours of seeker operation without a single failure.
- The program has augmented and refined the Integrated Flight System (IFS) model by incorporating the results of over 2,260 Captive Flight Test runs as well as weapon flight

tests. IFS model verification and validation is expected to be complete by the end of March 2017, and the Air Force Operational Test and Evaluation Center is expected to accredit it prior to the start of operational testing.
- The Program Office completed over 2,000 hours of ground reliability testing and nearly 200 hours of in-flight reliability testing.
- The program began a 28-shot NA mode GCT program in October 2016, which will test the weapon in more operationally realistic environments with operationally representative hardware and software. GCT will test the weapon versus maritime targets, countermeasures, and GPS-degraded environments.
- The Air Force awarded the $49 Million Low-Rate Initial Production Lot 2 contract on September 8, 2016, for 250 weapons.
- The Air Force conducted all testing in accordance with the DOT&E-approved Test and Evaluation Master Plan.

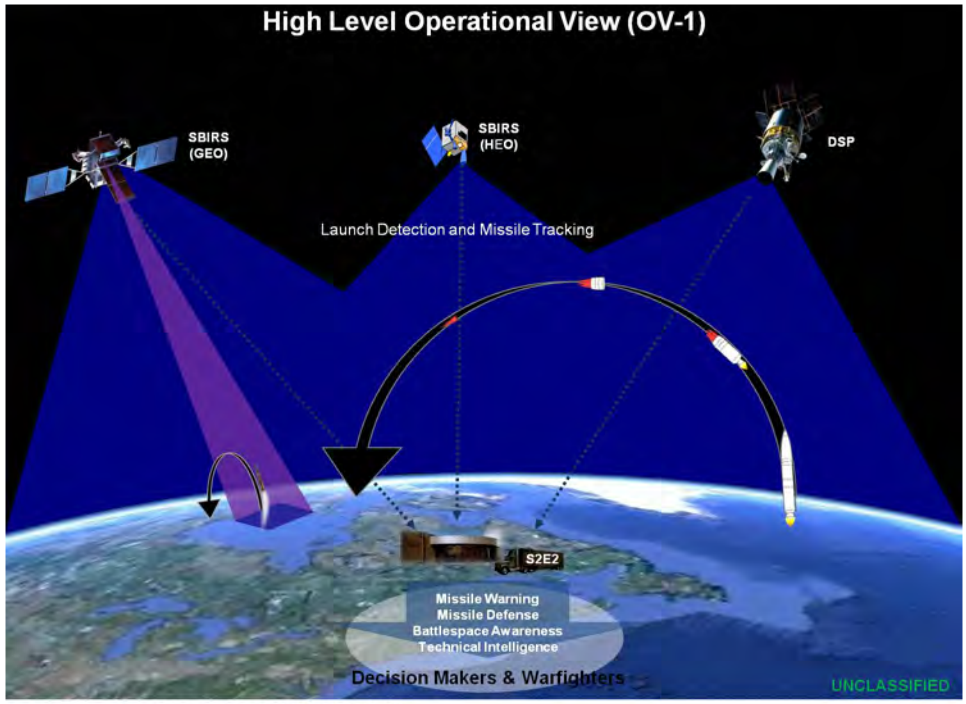
Assessment
- SDB II is progressing towards meeting its effectiveness, reliability, and lethality requirements in the NA mode, which is the primary employment method for SDB II. SDB II successfully engaged both moving and stationary targets, including proper classification of target type (wheeled versus track) on 15 of 19 GTV flight tests; 1 GTV struck the secondary target and 3 events had failures. The program has aggressively and thoroughly implemented corrective actions and fixes for all failure modes discovered in test.
- The SDB II Program Office is preparing for IOT&E with an adequately resourced test program and no unresolved major programmatic testing problems. IOT&E is scheduled to begin in 4QFY17.
- Three GTV missions and one LF mission required additional attempts and were successfully repeated after completion of the failure investigation and implementation of corrective actions. All corrective actions to date have been successful in preventing repeats of the observed failure modes. LF-5, which the Air Force conducted on September 14, 2015, did not detonate. The investigation was completed and corrective actions implemented. The test was successfully repeated along with two other remaining LF shots September 17, 2016, to assess the lethality of the SDB II.
- LF-10, which was attempted on October 3, 2016, detonated but failed to guide to the target. LF-10 was the first LF mission using LIA. The failure investigation is ongoing.
- The Air Force successfully completed two LIA tests and two CA attacks in 2016. A third CA test, CA-3, was conducted on May 19, 2016. The weapon successfully guided to the target, but the height-of-burst fuze functioned prematurely. The SDB II Program Office determined the likely root cause of the anomaly and implemented corrective action, which was successfully demonstrated on CA-2 in September 2016. The program has met the requirements to award Lot 2 of the contract.
- The Air Force successfully conducted the first GCT of SDB II on October 18, 2016, using NA versus a static target and demonstrated in-flight retargeting of the weapon.
- The weapon failed one environmental test related to the shipboard environment. The program implemented corrective action and successfully qualified design changes in corrosion, temperature, altitude and humidity, and vibration environments.
- Continued comparisons of the IFS model pre- and post-flight predictions indicate the model is adequate for the kinematics flown in-flight test to date. Raytheon Missile Systems will continue to develop and update the IFS model, which will be essential to the assessment of the results of live fire and operational testing. IFS, in combination with lethality data, will produce single shot kill probability values needed to assess end-to-end weapon effectiveness against a range of operationally relevant targets.
- The weapon is progressing towards demonstrating the required reliability by the start of IOT&E. Further testing in GCT, LF, and the Captive Carry Reliability Test program is expected to increase confidence in weapon reliability.

Recommendations
- Status of Previous Recommendations. The Air Force completed all previous recommendations.
- FY16 Recommendation.
  1. The Air Force should continue to use the results of GCT to further refine the IOT&E test plan.

Space-Based Infrared System Program, High Component (SBIRS HIGH)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted an Operational Utility Evaluation (OUE) of the Space-Based Infrared System (SBIRS) Increment 2, Block 10 from June 12 through August 30, 2016, in accordance with a DOT&E-approved test plan. Testing focused on the SBIRS ground architecture, and included two SBIRS geosynchronous Earth orbit (GEO) satellites, two hosted infrared payloads in highly elliptical orbit (HEO), and legacy Defense Support Program (DSP) satellites.
- DOT&E sent classified memoranda regarding cybersecurity issues discovered in OT&E to Air Force leaders.
- DOT&E is planning to publish a classified report on the OUE to inform Air Force employment and follow-on development decisions.



DSP - Defense Support Program
GEO - Space Based Infrared System (SBIRS) Geosynchronous Earth Orbiting Satellite
HEO - SBIRS Highly-Elliptical Orbit Payload
S2E2 - SBIRS Survivable/Endurable Evolution Program

System

- SBIRS is an integrated system of systems consisting of both survivable and non-survivable space and ground elements, designed to provide infrared sensing from space to support the DOD and other customers. SBIRS replaces or incorporates legacy DSP ground stations and satellites and is intended to improve upon DSP timeliness, accuracy, and threat detection sensitivity. SBIRS is being developed in two system increments.
  - Increment 1 used the SBIRS fixed-site ground Control Segment, operating with DSP satellites, to sustain legacy DSP military capability. The Air Force attained Initial Operational Capability for Increment 1 on December 18, 2001, consolidating the operations of the DSP and Attack and Launch Early Reporting to Theater systems.
  - At full capability delivery, Increment 2 will include a space segment consisting of two hosted payloads in HEO and four satellites in GEO, new Mission Control Station (MCS) fixed-site ground system software and hardware for consolidated data processing across all sensor families, and a new SBIRS Survivable Endurable Evolution (S2E2) mobile ground capability to replace the legacy Mobile Ground System (MGS). These Increment 2 capabilities are being delivered in multiple, discrete blocks, which each require dedicated test and evaluation.
    - SBIRS Increment 2, Block 10 has been delivered. Block 10 introduces new ground station software and hardware, enabling for the first time the integrated processing of DSP, GEO, and HEO sensor data at the MCS and MCS Backup (MCSB), and allowing the integration of GEO Starer sensor data.
    - SBIRS Increment 2, Block 20 and S2E2 remain in development.
      - Block 20 is scheduled for delivery in late 2018, and is intended to further improve ground station software at the MCS and MCSB. The software is intended to enable optimized sensor data clutter and background suppression to detect dimmer targets, and auto-cueing of GEO Starer sensors to provide better threat tracking and impact point prediction accuracy.
      - S2E2 is scheduled for delivery in late 2019.
  - The Air Force is currently operating two HEO payloads and two SBIRS GEO satellites on-orbit, and is preparing a third GEO satellite for launch. The Air Force will continue to launch additional GEO satellites to complete and sustain the SBIRS constellation over the next few years, and will use SBIRS Increment 2 to operate legacy DSP satellites until each is decommissioned, and to interoperate with MGS until S2E2 is delivered.

Mission

The Joint Functional Component Command for Space, a component of U.S. Strategic Command, employs SBIRS to provide reliable, unambiguous, timely, and accurate missile warning and missile defense information, as well as technical intelligence and battlespace awareness to the President of the United States, the SECDEF, Combatant Commanders, and other users.

Major Contractors

- Lockheed Martin Space Systems – Sunnyvale, California
- Northrop Grumman Electronic Systems – Azusa, California
- Lockheed Martin Information Systems and Global Solutions – Denver, Colorado

---

Activity

- AFOTEC conducted a SBIRS Block 10 dedicated OUE from June 12 through August 30, 2016, at Buckley and Schriever AFBs, Colorado, in accordance with the DOT&E-approved Enterprise Test and Evaluation Master Plan (ETEMP) and OUE test plan. Preceding the OUE and with DOT&E approval, AFOTEC collected operationally relevant effectiveness and suitability data for its OUE evaluation during the integrated test and evaluation conducted by the contractor and Air Force Program Office from January 30 through May 17, 2016.
  - AFOTEC conducted the OUE concurrently with an AFSPC Trial Period of operational use, in parallel with continued operation of the legacy SBIRS ground system. The OUE included both observed real-world mission performance against actual events, and use of accredited high-fidelity simulations of satellite sensor data and playbacks of previously recorded events to represent real-world scenarios.
  - AFOTEC has prepared a classified OUE report.
- DOT&E is planning to publish a classified test report on the OUE to inform Air Force employment and follow-on development decisions.
- The Air Force is drafting an update to the ETEMP for coordination in early 2017, which must incorporate test design refinements for a design of experiments-based OT&E for SBIRS Increment 2, Block 20 and SBIRS S2E2, including adequate threat representation and cybersecurity measures to complete a SBIRS survivability evaluation.

Assessment

- DOT&E sent classified memoranda regarding SBIRS cybersecurity issues discovered in OT&E to the Commanders of AFSPC, the Air Force Space and Missile Systems Center, and AFOTEC on May 19, 2016, and to the Secretary of the Air Force on June 27, 2016.
- DOT&E's classified OUE test report will include detailed effectiveness, suitability, and survivability assessments, as well as observations, detailed findings, and recommendations.

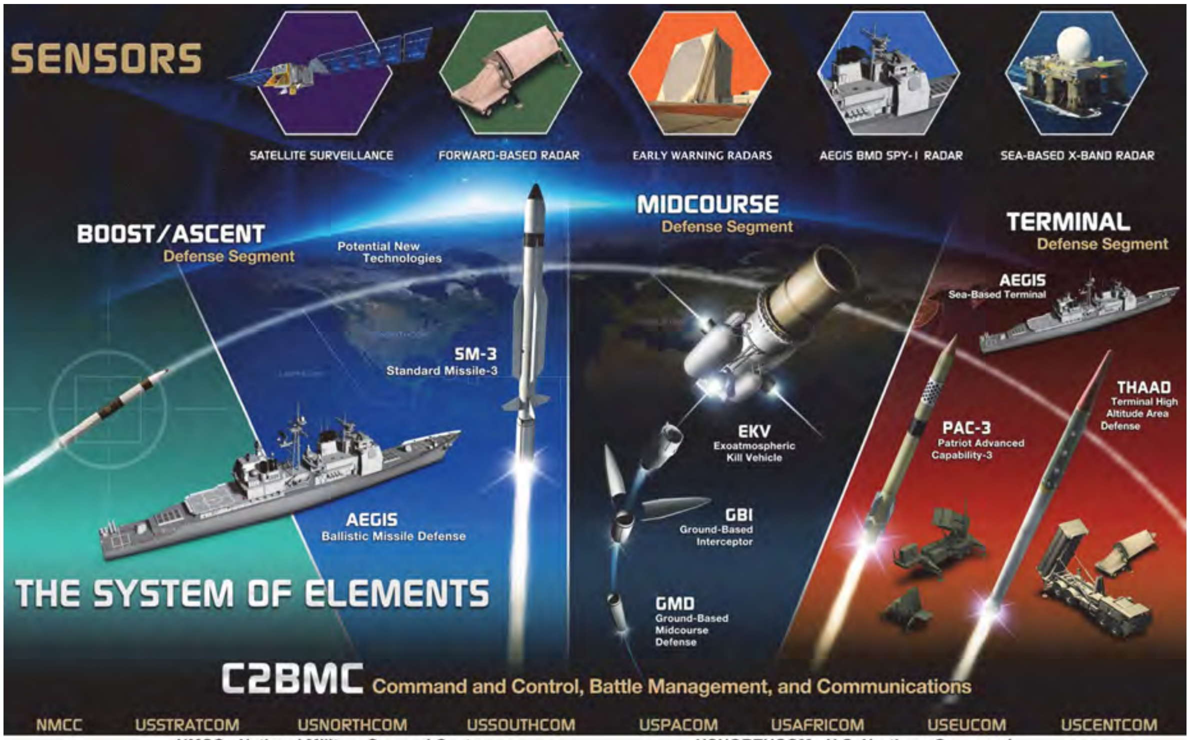
Recommendations

- Status of Previous Recommendations. The Air Force made significant progress on or satisfactorily addressed all nine previous recommendations contained in the FY12 Annual Report and the December 2012 classified DOT&E OUE report.
- FY16 Recommendations. The Air Force should:
  1. Fully resource dedicated cybersecurity personnel and tools to ensure active defense of SBIRS.
  2. Plan and execute Cooperative Vulnerability and Penetration Assessments (CVPAs) for cybersecurity in accordance with published DOT&E guidance. The Air Force should conduct the CVPAs with sufficient time prior to dedicated OT&E and the associated cybersecurity Adversarial Assessment to ensure the Air Force has the opportunity to correct or mitigate deficiencies identified during the CVPAs.
  3. Plan for adequate OT&E of SBIRS Block 20 and S2E2, including comprehensive threat representation and a thorough, rigorous design of experiments-based test design in accordance with published DOT&E guidance, to inform the operational acceptance and Full Operational Capability decisions for SBIRS Increment 2.

Ballistic Missile Defense Systems

Ballistic Missile Defense Systems

Ballistic Missile Defense System (BMDS)



NMCC - National Military Comand Center
USAFRICOM - U.S. Africa Command
USCENTCOM - U.S. Central Command
USEUCOM - U.S. European Command
USNORTHCOM - U.S. Northern Command
USPACOM - U.S. Pacific Command
USSOUTHCOM - U.S. Southern Command
USSTRATCOM - U.S. Strategic Command

Executive Summary

- No Homeland Defense intercept flight testing occurred in FY16. Hence, previous assessments that the Ballistic Missile Defense System (BMDS) demonstrates a limited capability to defend the U.S. Northern Command (USNORTHCOM) area of responsibility from small numbers of simple intermediate-range or intercontinental ballistic missile threats (greater than 3,000 km range) launched from North Korea or Iran remain unchanged.
- The Regional/Theater BMDS demonstrates a limited capability to defend the U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility for small numbers of medium- and intermediate-range ballistic missile threats (1,000 to 4,000 km), and a fair capability for short-range ballistic missile threats (less than 1,000 km range).
- The Flight Test, Operational-02 (FTO-02) Event 1a flight test demonstrated an Aegis Ashore remote engagement capability with Standard Missile-3 (SM-3) Block IB Threat Update (TU) guided missiles using data from an AN/TPY 2 Forward-Based Mode (FBM) radar. This was an important demonstration of the European Phased Adaptive Approach (EPAA) Phase 2 BMDS capability. The FTO-02 Event 2a flight test demonstrated a layered BMDS with multiple combat systems sharing common defended areas and shot opportunities against two threat-representative ballistic missiles.
- The Missile Defense Agency (MDA) conducted a non-intercept Homeland Defense flight test (Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+)) during which the MDA demonstrated the Capability Enhancement-II (CE-II) Exo-atmospheric Kill Vehicle (EKV) Alternate Divert Thrusters (ADTs) in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally, but the EKV experienced an anomaly unrelated to the new ADT system. The MDA collected extensive phenomenology data for discrimination improvements.
- The MDA completed the BMDS Capability Increment 6 System Requirements Review. Capability Increment 6 includes the Re-designed Kill Vehicle, Long Range Discrimination Radar, and discrimination improvements.
- Since FY10, DOT&E has assessed and reported annually that the lack of accreditation of models and simulation for performance assessment have limited DOT&E's use of these data for quantitative evaluations. This assessment remains unchanged for FY16. The MDA should increase

the development priority and associated funding for a BMDS high-fidelity, end-to-end, digital modeling and statistically significant simulation capability.
- The MDA also conducted several wargames and exercises designed to enhance Combatant Command ballistic missile defense (BMD) readiness and increase Service member confidence in the deployed elements of the BMDS.

System

The BMDS is a federated and geographically distributed system of systems that relies on element interoperability and warfighter integration for system-level operational effectiveness and efficient use of guided missile/interceptor inventory. BMDS includes five elements: four autonomous combat systems and one sensor/command and control architecture.

- Autonomous combat systems – Ground-based Midcourse Defense (GMD), Aegis BMD/Aegis Ashore Missile Defense System (AAMDS), Terminal High-Altitude Area Defense (THAAD), and Patriot
- Sensors – COBRA DANE radar, Upgraded Early Warning Radars (UEWRs), Sea Based X band (SBX) radar, AN/TPY 2 (FBM) radar, Aegis AN/SPY 1 radar aboard an Aegis BMD ship, and the Space-Based Infrared System (SBIRS)
- Command and control – Command and Control, Battle Management, and Communications (C2BMC)

Mission

- USNORTHCOM, USPACOM, USEUCOM, and USCENTCOM employ the assets of the BMDS to defend the United States, deployed forces, and allies against ballistic missile threats of all ranges.
- The U.S. Strategic Command synchronizes operational-level global missile defense planning and operations support for the DOD.

Major Contractors

- The Boeing Company
  - GMD Integration: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, and AN/SPY-1 radar: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado
  - SBIRS: Sunnyvale, California
  - THAAD Weapon System and Patriot Advanced Capability-3 Interceptors: Dallas, Texas
  - THAAD Interceptors: Troy, Alabama
- Northrop Grumman Corporation
  - GMD Fire Control and Communications: Huntsville, Alabama
- Orbital ATK
  - GMD Booster Vehicles: Chandler, Arizona
- Raytheon Company
  - GMD EKV and SM-3/6 Interceptors: Tucson, Arizona
  - Patriot Weapon System including Guidance Enhanced Missile-Tactical interceptors, AN/TPY-2 radar, COBRA DANE radar, SBX radar, and UEWRs: Tewksbury, Massachusetts

---

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The BMDS Operational Test Agency and the MDA conducted the FTO-02 Event 2a flight test in November 2015 at Wake Island and the broad-ocean area surrounding it. The primary test objective was to assess Aegis BMD system capability to prosecute a ballistic missile threat engagement in the presence of non organic post intercept debris, while simultaneously conducting anti-air warfare. The THAAD combat system, using Lot 4 interceptors for the first time, generated a non-organic post-intercept debris scene for Aegis BMD.
- The BMDS Operational Test Agency and the MDA executed the FTO-02 Event 1a flight test in December 2015 at the Pacific Missile Range Facility (PMRF) on Kauai, Hawaii. The test objective was to demonstrate the operational capability of the EPAA Phase 2 BMDS, anchored by the Aegis Ashore combat system, to defend Europe against medium-range ballistic missiles (MRBMs). The test was the first target intercept by the AAMDS and the first flight for the SM-3 Block IB TU guided missile.
- No Homeland Defense intercept flight testing occurred in FY16. The MDA conducted a non-intercept GM CTV 02+ flight test in January 2016 using GMD, the AN/TPY-2 (FBM) radar, the SBX radar, and C2BMC. This test was a demonstration of the CE-II EKV ADT and a discrimination phenomenology data collection.
- During FY16, the MDA conducted four system-level ground tests.
  - The Ground Test, Distributed-06 (GTD-06) Part 1 ground test, in October 2015, assessed BMDS-level theater/regional capabilities in USEUCOM's and USCENTCOM's area of responsibility in a distributed test environment.
  - The Ground Test, Integrated-06 (GTI-06) Part 2 ground test, in May 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in an integrated test environment.
  - The Ground Test, Integrated-Israel (GTI-ISR) (16) ground test, in July 2016, assessed the interoperability of Israeli and U.S. BMDS systems in an integrated test environment.
  - The GTD-06 Part 2 ground test, in September 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's areas of responsibility in a distributed test environment.

- The MDA completed the BMDS Capability Increment 6 System Requirements Review in May 2016. Capability Increment 6 includes the Redesigned Kill Vehicle, Long Range Discrimination Radar, and discrimination improvements.
- The MDA also conducted several wargames and exercises designed to enhance Combatant Command BMD readiness and increase Service member confidence in the deployed elements of the BMDS.

Assessment

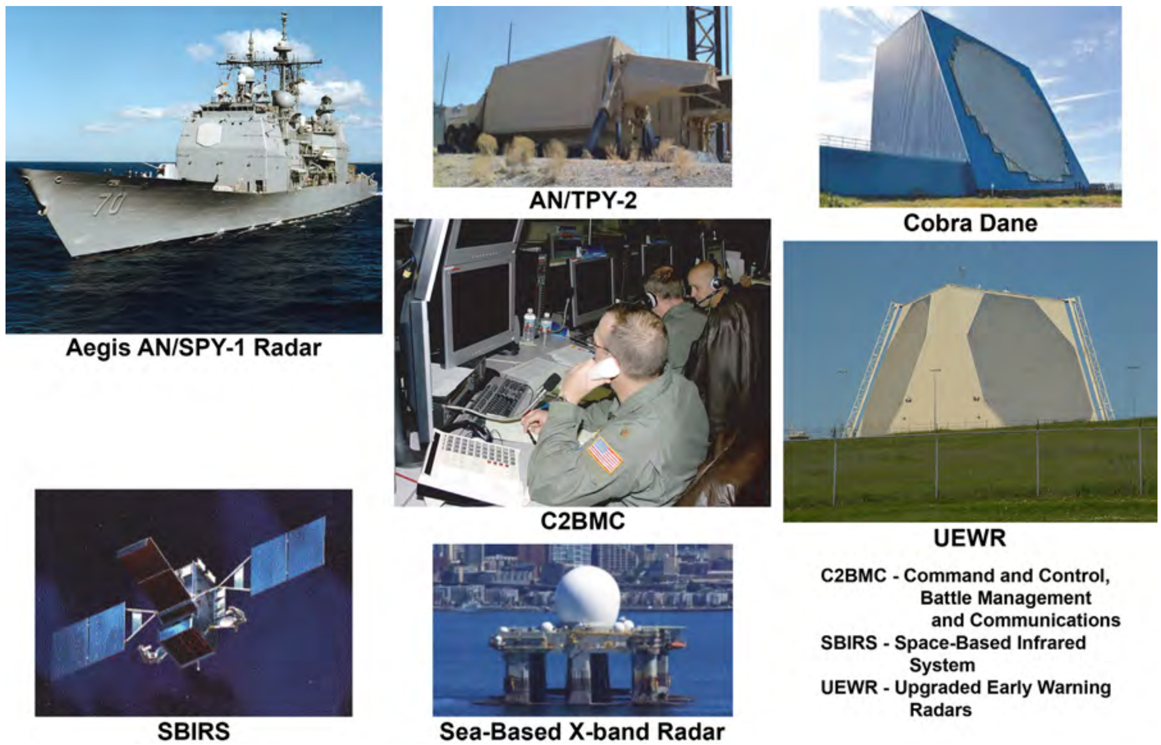
- The MDA, in collaboration with DOT&E, updated the Integrated Master Test Plan to incorporate BMDS element maturity, program modifications, and fiscal constraints.
- The FTO-02 Event 2a flight test demonstrated a layered BMDS with multiple combat systems sharing common defended areas and shot opportunities against two threat-representative ballistic missiles.
  - C2BMC software version S6.4-2.2.0 managed the AN/TPY-2 (FBM) radar, executed track reporting of sensor data to Link 16, and forwarded track data between the Aegis BMD and THAAD systems for subsequent engagements.
  - The THAAD combat system with version 2.7 software and using Lot 4 interceptors for the first time, intercepted a complex short-range ballistic missile target.
  - The Aegis BMD engaged an MRBM target. The Aegis Baseline 9.C1 destroyer operating in Integrated Air and Missile Defense radar priority mode engaged the target on remote track data from the AN/TPY-2 FBM CX-2.1.0 radar at Wake Island, and launched an SM-3 Block IB TU guided missile against the target. A faulty G-switch in the SM-3's guidance section failed early in the missile's flight, preventing a midcourse intercept. The malfunctioning G-switch precluded the separation of the missile's second stage from the first stage. A failure review board determined that the G-switch malfunctioned due to mechanical failure from abnormally high sticking in the component's lubricant. The program addressed the problem by implementing improved testing and screening of the G-switch before acceptance for installation. The new process changes were implemented and successfully flown in a controlled test flight.
  - Concurrently, the Aegis BMD ship successfully engaged a cruise missile surrogate target with an SM-2 Block IIIA guided missile.
  - THAAD also engaged the MRBM target and intercepted it.
- In FTO-02 Event 1a, sailors in the Aegis Ashore Missile Defense Test Facility at PMRF engaged an air-launched MRBM target using data from an AN/TPY-2 (FBM) CX 2.1.0 radar located at PMRF. This was an important demonstration of MRBM defense capability relevant to the EPAA Phase 2 BMDS and increased capability for theater/regional BMD. C2BMC relayed AN/TPY-2 (FBM) target track data to Aegis Ashore. Aegis Ashore fired an SM-3 Block IB TU guided missile on the remote track data, and intercepted a target for the first time. The firing assets consummated the engagement using local AN/SPY-1 radar data, rather than that of the AN/TPY-2 (FBM) radar. Although ground testing and unaccredited high-fidelity modeling and simulation have demonstrated all aspects of Aegis BMD's remote engagement capability, the lack of a flight test demonstration or data produced by accredited models reduces certainty in this capability.
- In both FTO-02 events, previously seen system network, radar track management, object discrimination and debris mitigation algorithms, and/or launch event association inaccuracies were noted again. The classified European Phased Adaptive Approach Phase 2 Operational Test and Evaluation Report and the 2015 Assessment of the BMDS report have additional assessment details and recommendations.
- During GM CTV-02+, the MDA demonstrated the CE-II EKV ADTs in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally, but the EKV experienced an anomaly unrelated to the new ADT system. See the GMD article for additional details. The MDA collected extensive phenomenology data for discrimination improvements.
- In GTD-06 Part 1, the MDA demonstrated interoperability between Aegis Ashore, Aegis BMD, THAAD, the AN/TPY-2 (FBM) radars, C2BMC, and SBIRS in scenarios against theater/regional threats in USEUCOM and USCENTCOM areas of responsibility. The MDA exercised the new capabilities of Aegis BMD software versions BL9.B1/C1, including new engagement planning functionality and an expanded threat set. These test data support the evaluation of BMDS and element-level interoperability and performance against SRBM and MRBM threats.
- In the GTI-06 Part 2 and GTD-06 Part 2 ground tests, the MDA demonstrated interoperability of the GMD GFC software version 6B3.1 with the SBIRS, UEWRs, C2BMC, AN/TPY-2 (FBM) radar, Aegis AN/SPY-1 radar in its long-range surveillance and track mode, the SBX radar, and Patriot Advanced Capability-3. The MDA evaluated a number of GMD software upgrades, including the discrimination logic, SBX tasking, and GFC salvo logic. These test data support the evaluation of GMD system performance against an expanded strategic threat set.
- BMDS-level integrated training capabilities for warfighter and interoperability functions remain limited. See the classified DOT&E European Phased Adaptive Approach Phase 2 Operational Test and Evaluation Report for additional assessment detail.
- The "integrated BMDS" refers to the full complement of BMDS combat systems that have a defensive capability for a given defended area, operating in a fully integrated fashion for the efficient use of the available interceptor inventory. The MDA has not yet demonstrated such an integrated BMDS capability. The MDA has demonstrated a basic BMDS combat capability that includes non-automated engagement planning and execution across the four threat classes (short-range, medium-range, intermediate-range, and intercontinental ballistic missiles) and in multiple phases of flight, but a

considerable amount of development is still necessary to field a robust, reliable, and fully integrated BMDS.
- In FY10, DOT&E reported, "the MDA began execution of its revamped Integrated Master Test Plan to collect the data needed to accredit the models and simulations used for assessing performance and effectiveness of the BMDS." Since then, DOT&E has assessed and reported annually that the lack of accreditation of models and simulation for performance assessment have limited DOT&E's use of these data for quantitative evaluations. This assessment remains unchanged for FY16.

Recommendations

- Status of Previous Recommendations. The MDA has addressed most previous BMDS recommendations. The following recommendations remain outstanding. The MDA should:
  1. Continue to address recommendations made in the DOT&E FTO-01 assessment found in the classified DOT&E February 2014 BMDS Annual Report, Appendix E.
  2. Increase the development priority and associated funding for the BMDS simulation-based performance assessment capability. The ability to produce high-fidelity and statistically significant BMDS level performance assessments is critical (FY14 Recommendation).
  3. Include Patriot in system-level operational flight test events in order to assess interoperability and integration between all of the BMDS combat systems and sensors. The MDA has completed initial design for flight tests in FY17-19 and has identified additional flight tests in FY20-22 to address this FY15 recommendation.
- FY16 Recommendations. The MDA should
  1. In conjunction with the Services, develop and implement integrated BMDS-level training in formal warfighter certification plans.
  2. Assess the performance of the BMDS in both flight and ground testing using realistic Link 16 loading and network configurations.
  3. Include the situational awareness tools used by the fire coordination and link management officers in their assessment of BMDS performance and ensure that warfighter involvement in testing is reflective of Combatant Command operations.
  4. Publish a comprehensive BMDS cybersecurity document that delineates the strategy for effective cybersecurity, achievable milestones for implementing the strategy, and stakeholder roles and responsibilities.
  5. Include reliability, maintainability, availability, and supportability data collectors for all participating elements in operationally realistic flight and ground test events to ensure that sufficient reliability, maintainability, availability, and supportability data are collected to allow for an assessment of operation suitability for all BMDS elements and sensors.
  6. Use targets with threat-representative reactive payloads in some future flight testing to improve the evaluation of lethality, sensor loading, battle management, and kill assessment.

Sensors / Command and Control Architecture



Executive Summary

- The Missile Defense Agency (MDA) continued to mature the Ballistic Missile Defense System (BMDS) sensors/command and control architecture. During FY16, the MDA used the sensor/command and control architecture in one Ground-based Midcourse Defense (GMD) developmental flight test, two BMDS operational flight tests, and four ground tests. Additionally, the Air Force used the sensor/command and control architecture in one intercontinental ballistic missile (ICBM) reliability and sustainment flight test.
- Many COBRA DANE radar system components and facilities are past the original design lifespan. Options for long-term supportability are diminishing and many of the original equipment manufacturers no longer exist. The Air Force awarded a $77 Million, 2-year contract to Raytheon for operations, maintenance, and sustainment of the COBRA DANE radar.
- The MDA demonstrated AN/TPY-2 Forward-Based Mode (FBM) radar capabilities, including enhanced tracking; improved debris mitigation and launch complex association algorithms; and updated discrimination and decision control logic.
- The Army continues to transition AN/TPY-2 (FBM) radar operations and maintenance from contractor logistics support to organic soldier operations and maintenance. Training and documentation deficiencies continue to be discovered, most recently in both Flight Test, Operational-02 (FTO-02) events. Soldiers are now responsible for activities at two of the five deployed radars.
- The MDA demonstrated Command and Control, Battle Management, and Communications (C2BMC) threat assessment, threat evaluation, sensor resource management, sensor track data processing, track reporting, target selection, discrimination and debris mitigation tasking, sensor/weapon access determination, and engagement monitoring during dedicated flight and ground testing as well as when tracking real-world ballistic missile targets-of-opportunity. C2BMC provided Combatant Commanders with timely and accurate information on numerous real-world events.
- The MDA awarded Lockheed Martin a $784.3 Million contract to develop and operate the Long Range Discrimination Radar.

System

- The BMDS sensors are systems that provide real-time ballistic missile threat data to the BMDS. The data are used to counter ballistic missile attacks. The sensor systems are operated by the Army, Navy, Air Force, and the MDA.
  - The COBRA DANE radar is a fixed site, single-face, L-band phased array radar operated by the Air Force and located at Eareckson Air Station (Shemya Island), Alaska.

  - The Upgraded Early Warning Radars (UEWRs) are fixed site, multiple-face, ultra-high frequency radars operated by the Air Force and located at Beale AFB, California (two radar faces); Fylingdales, United Kingdom (three radar faces); and Thule, Greenland (two radar faces). The MDA and Air Force Space Command are also upgrading the Early Warning Radars in Clear Air Force Station, Alaska (FY17), and Cape Cod Air Force Station, Massachusetts (FY18).
  - The Sea-Based X-band (SBX) radar is a mobile, phased array radar operated by the MDA and located aboard a twin-hulled, semi-submersible, self-propelled, ocean-going platform.
  - The AN/TPY-2 (FBM) radar is a transportable, single-face, X-band phased array radar commanded and tasked by the C2BMC, and located at sites in Japan, Israel, Turkey, and the U.S. Central Command (USCENTCOM) area of responsibility.
  - The list of BMDS sensors also includes the Aegis AN/SPY-1 radar and the Space-Based Infrared System (SBIRS)/Defense Support Program satellites. See the Aegis Ballistic Missile Defense (BMD) and SBIRS articles (pages 413 and 403, respectively), for reporting on these sensors.
- The C2BMC system is a Combatant Command interface to the BMDS. More than 70 C2BMC workstations are fielded at U.S. Strategic Command, U.S. Northern Command (USNORTHCOM), U.S. European Command (USEUCOM), U.S. Pacific Command (USPACOM), and USCENTCOM; numerous Army Air and Missile Defense Commands; Air and Space Operations Centers; and other supporting warfighter organizations.
  - The current C2BMC provides Combatant Commands and other senior national leaders with situational awareness of BMDS status, system coverage, and ballistic missile tracks by displaying selective BMDS data for strategic/national missile defense and for theater/regional missile defense, utilizing multiple message formats and diverse terrestrial and satellite communications paths.
  - The C2BMC also provides a consolidated upper echelon BMD mission plan at the Combatant Command and component level. BMDS elements (Aegis BMD, GMD, Patriot, and Terminal High-Altitude Area Defense (THAAD)) use their own command and control battle management systems and mission-planning tools for stand-alone engagements.
  - The current C2BMC S6.4 suite provides command and control for the AN/TPY-2 (FBM) radar as well as track reporting to support weapon system cueing and engagement operations.
  - Using the BMDS Communications Network, the C2BMC forwards AN/TPY-2 (FBM) and AN/SPY-1 tracks to GMD. C2BMC uses the Tactical Digital Information Link-Joint message formats to send C2BMC system track data to THAAD, Patriot, and coalition systems for sensor cueing and for Aegis BMD engagement support.
  - The C2BMC S8.2 (projected for FY17-18) is intended to mature and expand S6.4 capabilities as the next major step toward integrated, automated sensor management and engagement coordination.

Mission

- Combatant Commands use the BMDS sensors to detect, track, and classify/discriminate ballistic missile threats that target the United States and U.S. allies.
- Combatant Commands use C2BMC for deliberate and dynamic planning; situational awareness; track management; AN/TPY-2 (FBM) sensor management and control; engagement support and monitoring, data exchange between C2BMC and BMDS elements; and network management.

Major Contractors

- COBRA DANE Radar: Raytheon Company, Intelligence, Information, and Services – Dulles, Virginia
- UEWRs: Raytheon Company (Prime), Integrated Defense Systems – Tewksbury, Massachusetts; Harris Corporation/Exelis (Sustainment) – Colorado Springs, Colorado
- SBX, and AN/TPY-2 (FBM) Radars: Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts
- C2BMC: Lockheed Martin Corporation, Rotary and Mission Systems – Huntsville, Alabama, and Colorado Springs, Colorado

---

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- During FY16, the MDA and the Air Force used the sensor/command and control architecture in nine tests. The MDA executed one GMD developmental flight test, two BMDS operational flight tests, and four ground tests; the Air Force executed one ICBM reliability and sustainment flight test.
  - The FTO-02 Event 2a flight test, in October 2015, assessed a layered BMDS defense with multiple combat systems sharing common defended areas and shot opportunities.
  - The Ground Test, Distributed-06 (GTD-06) Part 1 ground test, in October 2015, assessed BMDS-level theater/regional capabilities in USEUCOM's and USCENTCOM's areas of responsibility in a distributed test environment.
  - The FTO-02 Event 1a flight test, in December 2015, assessed the operational capability of the regional/theater European Phased, Adaptive Approach Phase 2 BMDS, anchored by the Aegis Ashore Missile Defense System, to defend Europe against medium-range ballistic missiles.

- The Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+) flight test, in January 2016, assessed the Capability Enhancement-II Exo-atmospheric Kill Vehicle Alternate Divert Thruster performance in a flight environment while also assessing discrimination data flow through the fire control loop.
- The Ground Test, Integrated-06 (GTI-06) Part 2 ground test, in May 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in an integrated test environment.
- The Ground Test, Integrated-Israel (GTI-ISR) (16) ground test, in July 2016, assessed the interoperability of Israeli and U.S. BMDS systems in an integrated test environment.
- The GTD-06 Part 2 ground test, in September 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in a distributed test environment.
- The Glory Trip 219 flight test, in September 2016, is an Air Force Minuteman III ICBM reliability and sustainment assessment.

- The MDA used hardware-in-the-loop, training devices, and analytical models of the COBRA DANE radar, Beale UEWR, Thule UEWR, and Fylingdales UEWR during the GTI-06 Part 2 and GTD-06 Part 2 ground tests. In addition, the MDA used the Beale UEWR in the GM CTV-02+ flight test. The MDA also developed a COBRA DANE and Thule UEWR targets-of-opportunity campaign that will begin in FY17.
- The SBX radar was used in one GMD developmental flight test (GM CTV-02+), one ICBM reliability and sustainment flight test (Glory Trip 219), and two ground tests (GTI-06 Part 2 and GTD-06 Part 2).
- The MDA used the AN/TPY-2 (FBM) radar and C2BMC in one GMD developmental flight test (GM CTV-02+), two BMDS operational flight tests (FTO-02 Event 2a and FTO-02 Event 1a), and four ground tests (GTD-06 Part 1, GTI-06 Part 2, GTI-ISR (16), and GTD-06 Part 2). In addition, the Air Force used C2BMC and the AN/TPY-2 (FBM) radar in one ICBM reliability and sustainment flight test (Glory Trip 219).
- In January 2016, the MDA evaluated C2BMC Spiral 6.4 and AN/TPY-2 (FBM) in an Element Cybersecurity Experiment (ECE) to identify cybersecurity vulnerabilities with participation from Cyber Protection Team 800.
- In October 2015, the MDA awarded Lockheed Martin a $784.3 Million contract to develop and operate the Long Range Discrimination Radar. The MDA completed the System Requirements Review in February 2016.

Assessment

- During ground testing, the MDA gathered data to support evaluation of software upgrades and cybersecurity of the COBRA DANE radar, UEWRs, and the AN/TPY-2 and SBX radars, including verification that the COBRA DANE radar software upgrades resolved a technical issue related to scan-dependent biases.
- Many COBRA DANE radar system components and facilities are past the original design lifespan. Options for long-term supportability are diminishing, and many of the original equipment manufacturers no longer exist. In December 2015, the Air Force awarded a $77 Million, 2-year contract to Raytheon for operations, maintenance, and sustainment of the COBRA DANE radar.
- The ground test data showed mixed UEWR performance with several new missile threat objects added to the UEWR object classification database.
- The MDA demonstrated AN/TPY-2 (FBM) radar software upgrades, including enhanced tracking; improved debris mitigation and launch complex association algorithms; and updated discrimination and decision control logic.
- The MDA and the Army continue working to achieve full materiel release of the AN/TPY-2 (FBM) radar. Of the nine original materiel release conditions the Army created in 2012, the Army closed seven by 2014 and migrated the remaining two to the set of materiel release conditions associated with software version CX-1.2.3_18. Of the 25 CX 1.2.3_18 materiel release conditions, the Army closed one prior to 2016 and the Army closed four in 2016. The Army is also in the process of establishing additional materiel release conditions for software version CX-2.1.0.
- The Army continues to transition AN/TPY-2 (FBM) radar operations and maintenance from contractor logistics support to organic soldier operations and maintenance. Training and documentation deficiencies continue to be discovered, most recently in both FTO-02 events. Soldiers are now responsible for activities at two of the five deployed radars.
- In Glory Trip 219, the SBX radar acquired and tracked the Minuteman III ballistic missile through the boost and/or midcourse phases of flight.
- The MDA demonstrated C2BMC threat assessment, threat evaluation, sensor resource management, sensor track data processing, track reporting, target selection, sensor/weapon access determination, and engagement monitoring during dedicated flight and ground testing, as well as during real-world ballistic missile targets-of-opportunity.
  - The system demonstrated dual radar management and track processing/reporting utilizing operational C2BMC suites and communications.
  - The C2BMC engagement planner provided non-real-time performance analysis of the composition and location of U.S. and allied BMD assets, but does not currently provide a system-level capability to coordinate engagement decisions.
  - Software version S6.4-3.0 provided discrimination tasking of the AN/TPY-2 (FBM) radar for long-range threats, multiple-radar discrimination tasking of a threat, and several fixes related to message sequencing and timing.
  - During GM CTV-02+, the MDA used passive links to conduct real-time activities with upcoming C2BMC version S8.2 and to collect data on closed loop fire control, enhanced tracking, post intercept assessment, and discrimination.

- During FTO-02 Event 1a, C2BMC demonstrated support to Aegis BMD Launch on Remote via track processing of AN/TPY-2 data, system track formation, system track selection, and Link 16 track reporting.
- Flight testing with C2BMC control of two AN/TPY-2 (FBM) radars has yet to occur. However, C2BMC did exercise dual radar management, precision cueing, and system track formation during a dedicated ground test (USEUCOM and USCENTCOM areas of responsibility) and during real-world targets of opportunity (USPACOM and USEUCOM areas of responsibility).
- C2BMC has not demonstrated real-time engagement direction capabilities.

• Problems previously discovered during testing, if not corrected, could adversely affect C2BMC effectiveness. These problems, the details of which can be found in DOT&E's classified 2015 Assessment of the BMDS, include:
  - Track management and track processing problems
  - Data management problems

Recommendations

• Status of Previous Recommendations. The MDA has addressed all but two previous recommendations for the sensors/command and control architecture. The MDA:
  1. Made progress on sensor/command and control architecture cybersecurity testing by performing basic testing and system scans during GTI-06 Part 2 and one ECE. The MDA should continue to increase the number of components and the fidelity of its cybersecurity assessments.
  2. Has initiated, but not completed, a study on the additional sensor requirements for an effective defense of Hawaii.

• FY16 Recommendations. The MDA should:
  1. With the Air Force, identify spare and replacement part sources for long-term COBRA DANE radar sustainment.
  2. With the Army, update AN/TPY-2 (FBM) Interactive Electronic Technical Manuals and improve AN/TPY-2 (FBM) radar operator training.
  3. Perform a flight test with multiple AN/TPY-2 (FBM) radars to assess the ability of C2BMC to correctly task and fuse track data from multiple sources observing realistic targets and to assess the ability to disseminate the subsequent system-level data across the BMDS. Additionally, the MDA should evaluate BMDS performance in dual radar missions, particularly Defense of Europe for USEUCOM and Homeland Defense for USNORTHCOM, using the COCOM suite (which can only manage one radar), when the C2BMC Global Engagement Manager is non-mission capable.
  4. Continue C2BMC development efforts to provide an engagement management capability to the BMDS.

Aegis Ballistic Missile Defense (Aegis BMD)

Executive Summary

- The Missile Defense Agency (MDA) conducted three Aegis Ballistic Missile Defense (BMD) intercept flight tests in FY16. Overall, Aegis BMD successfully engaged two ballistic missile targets and one anti-air warfare target and failed to intercept one ballistic missile target.
- The MDA conducted operational flight testing of the Aegis Baseline 9.1 system (i.e., Aegis BMD 5.0 Capability Upgrade) in its Aegis Ashore (Baseline 9.B1) and Aegis destroyer (Baseline 9.C1) configurations with Standard Missile-3 (SM-3) Block IB Threat Upgrade (TU) guided missiles. Additionally, the MDA conducted developmental flight testing of the SM-3 Block IB TU guided missile and Sea-Based Terminal (SBT) capability.
- Although the program completed FOT&E for Aegis BMD 3.6.1 and IOT&E for Aegis BMD 4.0 in FY11 and FY15, respectively, the program continued to use system variants (i.e., Aegis BMD 3.6.3 and 4.0.3) in flight and ground tests and a U.S. Navy Fleet exercise in FY16 to assess element- and system-level engagement capabilities, long range surveillance and track (LRS&T) capabilities, and interoperability with the BMDS and foreign missile defense assets.
- During one of the five live-guided missile tests conducted in FY16, the SM-3 Block IB TU missile failed to launch from the Aegis BMD ship.
- The MDA conducted two developmental flight tests and six design verification and qualification ground test firings of the SM-3 Block IB TU Third Stage Rocket Motor (TSRM) to verify an aft nozzle area re-design that improves missile reliability.
- Testing demonstrated engagement capabilities against short and medium-range ballistic missiles (SRBM/MRBM) in both endo- and exo-atmospheric engagements and against anti-air warfare targets.
- Flight testing, modeling and simulation (M&S), and ground testing have demonstrated Aegis BMD capabilities to perform LRS&T.
- During integration testing of an SM-3 Block IIA flight test round, the Kinetic Warhead's guidance unit experienced a failure.
- Operational Aegis BMD assets and hardware-in-the-loop (HWIL) facilities underwent cybersecurity testing.
- The MDA deployed an Aegis Ashore site to Romania, and the U.S. European Command (USEUCOM) declared it operational.

System

- Aegis BMD is a sea- and land-based missile defense system that employs the multi-mission shipboard Aegis Weapon System, with improved radar and new missile capabilities to engage ballistic missile threats. Capabilities of Aegis BMD include:
  - Computer program modifications to the AN/SPY-1 radar for LRS&T of ballistic missiles of all ranges
  - A modified Aegis Vertical Launching System, which stores and fires SM-3 Block IA and Block IB guided missiles, modified SM-2 Block IV guided missiles, and SM-6 Dual I guided missiles
  - SM-3 Block IA and Block IB guided missiles that use maneuverable kinetic warheads to accomplish midcourse engagements of SRBMs, MRBMs, and intermediate-range ballistic missiles (IRBMs)
  - Modified SM-2 Block IV guided missiles that provide terminal engagement capability against SRBMs and MRBMs
  - SM-6 Dual I guided missiles that provide SBT capability against SRBMs and MRBMs in their terminal phase of flight, anti-ship cruise missiles, and all types of aircraft
- Aegis Ashore (Baseline 9.B1) is a land-based version of Aegis BMD, with an AN/SPY-1 radar and Vertical Launching System to enable engagements against MRBMs and IRBMs with SM-3 guided missiles. The first Aegis Ashore site in Romania is the central, land-based component of the second phase of the European Phased-Adaptive Approach (EPAA) for the defense of Europe.
- Aegis BMD ships and Aegis Ashore are capable of performing missile defense operations and sending/receiving cues to/from other BMDS sensors through tactical datalinks. Aegis BMD ships are capable of performing autonomous missile defense operations while both Aegis BMD ships and Aegis Ashore are capable of performing engagements using remote track data from BMDS sensors.

Aegis Cruiser   Aegis Ashore and Vertical Launch System

Mission

The Navy can accomplish three missile defense-related missions using Aegis BMD:

- Defend deployed forces and allies from short- to intermediate range theater ballistic missile threats

- Provide forward-deployed radar capabilities to enhance defense against ballistic missile threats of all ranges by sending cues or target track data to other BMDS elements
- Provide ballistic missile threat data to the Command and Control, Battle Management, and Communications (C2BMC) system for dissemination to Combatant Commanders' headquarters to ensure situational awareness

Major Contractors

- Aegis BMD Weapon System: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- AN/SPY-1 Radar: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- SM-3, SM-2 Block IV, and SM-6 Dual I Missiles: Raytheon Company, Missile Systems – Tucson, Arizona

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- In FY16, the MDA conducted operational flight testing of the Aegis Baseline 9.1 system in its Aegis Ashore (Baseline 9.B1) and Aegis destroyer (Baseline 9.C1) configurations with SM-3 Block IB TU guided missiles and conducted developmental flight testing of SBT capability.
- Although the program completed FOT&E for Aegis BMD 3.6.1 and IOT&E for Aegis BMD 4.0 in FY11 and FY15, respectively, the program continued to use system variants (i.e., Aegis BMD 3.6.3 and 4.0.3) in flight tests, system-level tests, and a U.S. Navy Fleet exercise in FY16 to assess element- and system-level engagement and LRS&T capabilities and interoperability with the BMDS and foreign missile defense assets.
- The MDA conducted three Aegis BMD intercept flight tests in FY16. Overall, Aegis BMD successfully engaged two ballistic missile targets and one anti-air warfare target and failed to intercept one ballistic missile target.
  - In October 2015, Aegis BMD participated in At-Sea Demonstration-15, a multi-event fleet exercise conducted in the United Kingdom's Hebrides Missile Range wherein assets from NATO member countries exchanged air and ballistic missile message information across operational communication architectures during cruise missile and ballistic missile engagements. In one of the nine exercise events, an Aegis BMD 3.6.3 destroyer with an SM-3 Block IA guided missile engaged and intercepted a non-separating SRBM target. Participating assets also included an Aegis BMD 3.6.3 laboratory representation, an Aegis 5.3.10 air defense ship, C2BMC, and Allied naval vessels from Great Britain, Spain, Netherlands, Italy, Canada, France, and Norway.
  - In November 2015, an Aegis Baseline 9.C1 destroyer operating in Integrated Air and Missile Defense (IAMD) radar priority mode participated in Flight Test Operational (FTO)-02 Event 2a at Wake Island and the broad-ocean area surrounding it. The MDA and BMDS Operational Test Agency (OTA) designed the test mission to demonstrate a layered BMDS with Aegis BMD and Terminal High-Altitude Area Defense (THAAD) sharing common defended areas and shot opportunities against two threat-representative ballistic missile targets. The primary Aegis BMD test objective was to prosecute a ballistic missile engagement in the presence of non-organic post-intercept debris generated by a THAAD intercept, while simultaneously conducting anti-air warfare against an anti-ship cruise missile surrogate. However, the SM-3 missile failed in flight, preventing a midcourse intercept of the ballistic missile target, while the Aegis BMD ship did successfully engage the cruise missile surrogate with an SM-2 Block IIIA guided missile. The MDA initially attempted to conduct this test in October 2015 as FTO-02 Event 2; however, due to a THAAD target malfunction, the October event was a "No Test."
  - In December 2015, the OTA and the MDA conducted FTO-02 Event 1a at the Pacific Missile Range Facility (PMRF) on Kauai, Hawaii. The test intended to demonstrate the operational capability of the EPAA Phase 2 BMDS, anchored by the Aegis Ashore combat system, to defend Europe against MRBMs. In the test, the Aegis Ashore Missile Defense Test Complex at PMRF engaged an air-launched MRBM target with an SM-3 Block IB TU guided missile using data from an AN/TPY-2 (Forward-Based Mode (FBM)) radar located at PMRF. This was the first intercept flight test for Aegis Ashore.
- Aegis BMD participated in two live-target and five live-guided missile test events in FY16. During one of the live-guided events, the SM-3 Block 1B TU missile failed to launch from the Aegis BMD ship.
  - In December 2015, the MDA conducted Aegis Ashore Control Test Vehicle-02 (CTV-02), a guided missile-only firing of an SM-3 Block IB TU missile. The MDA conducted this live-fire event as a risk reduction flight for FTO-02 Event 1a.
  - In December 2015, the MDA conducted Standard Missile Cooperative Development CTV-02, a guided missile-only, developmental flight test of the SM-3 Block IIA missile through nosecone deployment and kinetic warhead ejection. This was the second live-fire event for the SM-3 Block IIA guided missile, which is a joint U.S.-Japanese development of a 21-inch diameter variant of the SM-3.
  - In February 2016, the MDA conducted Standard Missile CTV-01, planned to be the first of two guided missile-only firings to verify the re-designed SM-3 Block IB TU TSRM aft nozzle area. The SM-3 Block IB TU missile failed to launch from the Aegis BMD 3.6.3 destroyer.

  - In May 2016, the MDA conducted SM CTV-01a, a re-test of SM CTV-01. An Aegis BMD 3.6.3 destroyer fired an SM-3 Block IB TU guided missile against a simulated test target to exercise a two-pulse firing of the TSRM using a minimum inter-pulse delay between the TSRM axial thrust burns. This was the first SM-3 Block IB firing from an Aegis BMD 3.6.3 ship.
  - In May 2016, the MDA conducted SM CTV-02. An Aegis BMD 3.6.3 destroyer fired an SM-3 Block IB TU guided missile against a simulated test target to exercise a two-pulse firing of the TSRM using a maximum inter-pulse delay between TSRM axial thrust burns.
  - In May 2016, the MDA conducted Flight Test Other-21 (FTX-21), planned to demonstrate the ability of an Aegis Baseline 9.C1-configured destroyer to detect and track an MRBM target within the Earth's atmosphere. The test was a risk reduction exercise for the future Flight Test Standard Missile (FTM)-27 flight test mission, which is planned for 1QFY17.
  - In June 2016, the Navy conducted Pacific Dragon, a Commander, Pacific Fleet-directed exercise. An Aegis Baseline 9.C2-equipped ship performed a simulated SM-3 Block IIA engagement against a separating MRBM target. This exercise served as risk reduction for the future Standard Missile Cooperative Development Project Flight Test Standard Missile-01 (SFTM-01) flight test mission and explored interoperability between U.S. Navy forces and naval assets from Japan and the Republic of Korea.
- Aegis BMD provided HWIL representations for four BMDS ground tests that provided information on Aegis BMD interoperability and functionality in various regional/theater scenarios:
  - GTD-06 Part 1 in October 2015 examined defense of USEUCOM and U.S. Central Command scenarios, using Aegis Baseline 9.B1 (Aegis Ashore Missile Defense System in Romania), Baseline 9.C1, Aegis BMD 4.0.3, and Aegis BMD 3.6.3.
  - GTI-06 Part 2 in April 2016 examined defense of U.S. Pacific Command and Homeland defense scenarios, using Aegis Baseline 9.C1, Aegis BMD 4.0.3, and Aegis BMD 3.6.3.
  - GTI-Israel-16 in June 2016 studied interoperability between the BMDS and the Arrow Weapon System for maintaining shared situational awareness, using Aegis BMD 4.0.3 and Baseline 9.C1.
  - GTD-06 Part 2 in September 2016 again examined defense of U.S. Pacific Command and Homeland defense scenarios, using Aegis BMD 3.6.3, Aegis BMD 4.0.3, and Aegis Baseline 9.C1.
- During integration testing of an SM-3 Block IIA flight test round, in preparation for SFTM-01, the MDA discovered a problem with the Kinetic Warhead's Guidance Unit.
- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted high-fidelity digital M&S runs using accredited models in support of Aegis Baseline 9.B1 in September 2016.
- COTF conducted a cybersecurity Adversarial Assessment of Aegis Baseline 9.B1 in June 2016 at the Aegis Ashore Missile Defense Facility in Romania. The Adversarial Assessment was the first cybersecurity assessment conducted on the Aegis Ashore Missile Defense System.
- USEUCOM declared the Aegis Ashore Missile Defense System in Romania operational in July 2016.

Assessment

- The Aegis BMD 4.0 system, which is the latest, widely deployed version of Aegis BMD and the primary sea-based firing asset for EPAA Phase 2, participated in HWIL and distributed ground test events in FY16 primarily to demonstrate LRS&T improvements in support of Ground-based Midcourse Defense (GMD) with the Aegis BMD 4.0.3 update.
- Prior IOT&E flight testing and supporting M&S demonstrated that Aegis BMD 4.0 has the capability to engage and intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase with SM-3 Block IB guided missiles. However, flight testing and M&S are not yet sufficient to assess the full range of expected threat types, ground ranges, and raid sizes. Details on Aegis BMD 4.0 performance can be found in the classified December 2014 Aegis BMD 4.0 IOT&E Report.
- In FY16, Aegis Baseline 9.B1 and Baseline 9.C1 underwent operational flight testing of those systems' remote engagement capabilities with SM-3 Block IB TU guided missiles using data from an AN/TPY-2 (FBM) radar (during FTO-02 Events 2a and 1a). The successful intercept in FTO-02 Event 1a by the Aegis Ashore Missile Defense Test Complex at PMRF demonstrated an MRBM defense capability relevant to EPAA Phase 2. During FTO-02 Event 2a, the SM-3 failed in flight; however, this event contributed tracking and engagement processing data relevant to an assessment of Aegis BMD's remote engagement capabilities. Similar to previous tests with remote engagements (FTM-15 in FY11 and FTM-20 in FY13), the system did not use remote AN/TPY-2 (FBM) radar data throughout the engagement. Instead, the firing assets consummated the engagement using local AN/SPY-1 radar data. Although Aegis BMD HWIL, distributed ground testing, and unaccredited high-fidelity M&S have demonstrated all remote engagement modes, the lack of a flight test demonstration of a fully remote engagement reduces certainty in that capability. High-fidelity digital M&S run results using accredited models in support of Aegis Baseline 9.B1 will be available 1QFY17 to support future assessments.
- In FTO-02 Event 2a, the SM-3 Block IB TU guided missile failed early in flight due to a faulty G-switch in the guidance section of the missile. The malfunctioning G-switch precluded the separation of the missile's second stage from the first stage. A failure review board (FRB) determined that the G-switch malfunctioned due to mechanical failure caused by abnormally high sticking in the component's lubricant. The program implemented improved testing and screening of the G-switch

before acceptance for installation to address the problem. The MDA implemented the new process changes prior to the successful SM CTV-01a and -02 flight tests.

- The MDA demonstrated the efficacy of the SM-3 Block IB TU re-designed TSRM aft nozzle area, to improve missile reliability following the FTM-16 Event 2 (FY11) and FTM-21 (FY13) failures during two flight tests (SM CTV-01a and -02) and six design verification and qualification ground test firings.
- Additional SM-3 Block IB component anomalies have occurred in recent flight and lot acceptance testing, one resulting in a failed SM-3 launch.
  - Low TSRM Attitude Control System cold gas regulator (CGR) pressures were observed in FTM-25 (FY15) and during lot acceptance testing. The CGR anomaly in FTM-25 did not preclude the target from being intercepted; however, the cold gas pressure observed was much lower than that commanded. If the regulated pressure from the CGR is too low, the Attitude Control System may not function properly. The Prime Contractor (Raytheon Missile Systems) established an FRB, which determined that now-defunct tooling procedures caused the FTM-25 CGR anomaly. The FRB determined that changes to the CGR C-seal's spring dimensions, additional inspections, and an enhanced acceptance test process addressed the low pressure anomalies from the lot acceptance tests.
  - A second anomaly was observed during SM CTV-01 when an SM-3 Block IB TU failed to launch due to the missile failing a pre-launch booster nozzle response built-in test designed to ensure safe missile egress from the firing ship. An FRB determined that random minor voltage glitches in guidance section components caused short-duration (tens of milliseconds) corrupted commands to be sent to the booster nozzle, which resulted in a failure of the built-in test. To address the problem, the program developed software that mitigates the possibility of failure by introducing logic to re-send commands up to two additional times. The new software was successfully flown in SM CTV-01a and -02, and will be installed on new production rounds.
  - Third, lot acceptance testing revealed a number of SM-3 Block IB TU kinetic warhead guidance units that were unresponsive at power up. An FRB established the root cause to be related to memory management during boot up. The MDA has implemented a minor change to the kinetic warhead's guidance unit software to correct the anomaly. These two software changes will be loaded on all Block IB TU missiles at their 4-year recertification periods.
- The successful simulated engagement in the Pacific Dragon Fleet exercise demonstrated the organic engagement capabilities of the Baseline 9.C2 system.
- The FTX-21 flight mission demonstrated the endo-atmospheric tracking capabilities of the Aegis Baseline 9.C1 system, which are relevant for the SBT engagement mission; however, no SBT engagements were attempted in FY16. To date, intercept testing of the Baseline 9.C1's SBT capabilities consists of the first two multi-mission warfare events in FY15. These events demonstrated that SM-6 Dual I and SM-2 Block IV missiles can be used to conduct SBT engagements against non-separating SRBMs, but high-fidelity M&S analyses conducted using models accredited by the BMDS OTA have not yet occurred, so SBT engagement performance cannot be quantitatively evaluated. Completion of a subset of the SBT M&S analyses is expected in 1QFY17.
- The MDA demonstrated Aegis Baseline 9.C1 system's IAMD capabilities to a limited degree in FTO-02 Event 2a, when the firing ship performed a remote ballistic missile engagement with the system operating in IAMD radar priority mode while conducting an anti-air warfare engagement against a single cruise missile surrogate. The demonstration of IAMD capabilities in FTO-02 Event 2a was not stressing, even less so than during FTM-25 (FY15), where a raid of two cruise missiles and a single ballistic missile target were simultaneously engaged in an organic engagement.
- Reliability, maintainability, availability, and supportability (RMA&S) data collected during Aegis Baseline 9.1 BMD-related testing through FY15 show that the system has lower than desired software stability. Also, the data show that the system does not currently meet its requirements for availability and mean time to repair hardware, mostly due to a series of early Aegis Display System failures and an AN/SPY-1 radar coolant leak that downed the system for an extended period of time. The majority of the Aegis Display System problems have since been addressed with the installation of new console graphics cards. DOT&E will reassess RMA&S once the MDA completes FTM-27 planned for December 2016.
- ASD-15 demonstrated Aegis BMD 3.6.3 retention of Aegis BMD 3.6.1 midcourse engagement capabilities against non-separating SRBMs, when an Aegis BMD 3.6.3 ship detected, tracked, and intercepted an SRBM using an SM-3 Block IA guided missile. ASD-15 also demonstrated that Aegis BMD can interoperate with NATO defenses and exchange air and ballistic missile message information across operational communication architectures during cruise missile and ballistic missile engagements. The MDA further demonstrated Aegis BMD 3.6.3 capabilities in FY16 during SM CTV-01a and -02, when an Aegis BMD 3.6.3 destroyer fired SM-3 Block IB TU missiles for the first time. Aegis BMD 3.6.3 is the only variant of the Aegis BMD 3.6 system that can fire SM-3 Block IB missiles.
- The MDA continues to utilize Aegis BMD assets and HWIL representations in ground test events and warfighter simulation exercises during operational flight test campaigns (e.g. FTO-02), which has helped to refine tactics, techniques, and procedures (TTPs) and overall interoperability of the system with the BMDS. However, the test events routinely demonstrated that inter-element coordination and interoperability need improvement. The tests highlighted multiple classified suitability and effectiveness shortfalls.
- The MDA continues to participate in tests of opportunity like the Pacific Dragon exercise, which provide a venue to explore interoperability between Aegis BMD assets and foreign ballistic missile defense assets. In Pacific Dragon, Aegis BMD

successfully exchanged data with Allied units from Japan and the Republic of Korea.

- Following the integration testing failure of an SM-3 Block IIA flight test round, the MDA initiated a Failure Investigation Team process and developed a fault tree. The flight test round will be disassembled and will undergo further analysis to determine the root cause of the failure.
- Cybersecurity testing results from the Adversarial Assessment of the Aegis Ashore Missile Defense Facility in Romania will be included in DOT&E's classified 2016 BMDS Annual Report to Congress.
- Testing has uncovered a number of classified survivability problems, which will be discussed in DOT&E's classified 2016 BMDS Annual Report to Congress.

Recommendations

- Status of Previous Recommendations. The program:
  1. Addressed the first recommendation from FY13 to conduct flight testing of the Aegis BMD 4.0 remote engagement authorized capability against an MRBM or IRBM target using SM-3 Block IB guided missiles, when it conducted FTO-02 Events 1a and 2a using Aegis Baseline 9.1 (BMD 5.0 Capability Upgrade) firing assets.
  2. Partially addressed the second recommendation from FY13, to conduct operationally realistic testing that exercises Aegis BMD 4.0's improved engagement coordination with THAAD and Patriot, when it conducted FTO-02 Event 2a using an Aegis Baseline 9.C1 destroyer and THAAD firing assets. This flight test did not include Patriot.
  3. Addressed the second recommendation from FY14, to determine the appropriate LRS&T TTPs for the transmission and receipt of Aegis BMD 4.0 track data for GMD use. GTI-06 Part 3 (FY15), GTI-06 Part 2, and GTD-06 Part 2 demonstrated that GMD can use data provided by Aegis BMD 4.0.3.
  4. Partially addressed the third recommendation from FY14, to ensure that sufficient flight testing of the Aegis Baseline 9.C1 system is conducted to allow for verification, validation, and accreditation (VV&A) of the M&S suite to cover the full design to Aegis BMD battlespace. Flight testing conducted in FY15 and early FY16 provided additional VV&A data, but the BMDS OTA has not yet accredited the high fidelity M&S suite.
  5. Addressed the fourth recommendation from FY14, to conduct sufficient ground and flight testing of the redesigned insulation components in the SM-3 Block IB TSRM nozzle to prove the new design works under the most stressing operational flight conditions. This occurred when the program completed a series of six design verification and qualification ground test firings and the SM CTV-01a and CTV-02 flight tests.
  6. Addressed the first recommendation from FY15, to use an industry-led FRB process to identify the root cause of low cold gas pressure anomalies observed in lot acceptance testing of the SM-3 Block IB CGR, and determine the appropriate corrective actions needed to ensure proper functioning. The FRB process determined that changes to the CGR C-seal's spring dimensions, additional inspections, and an enhanced acceptance test process were required and a follow-on study is underway to investigate the possibility of re-designing the CGR seal.
  7. Has not addressed the second recommendation from FY15, to conduct stressing simultaneous air and ballistic missile defense engagements with the Aegis Baseline 9.C1 system operating in IAMD radar priority mode, with multiple ballistic missiles and anti-ship cruise missile threats being simultaneously engaged.
  8. Has not addressed the third recommendation from FY15, to perform high-fidelity M&S analysis over the expected Aegis Ashore engagement battlespace for EPAA Phase 2 to allow for a broad quantitative evaluation of engagement capability. The MDA plans to complete the high-fidelity M&S analysis in FY18.
- FY16 Recommendations. The MDA should:
  1. Conduct high-fidelity M&S runs-for-the-record for the Aegis Baseline 9.2 system (Aegis BMD 5.1) to assess performance across the expected engagement battlespace in all Combatant Commands' Areas of Responsibility and develop an appropriate M&S VV&A plan to support that effort.
  2. Conduct a live-flight test demonstration of a fully remote engagement.
  3. Include BMDS OTA RMA&S data collectors in all flight test missions to improve the accuracy and statistical confidence of future suitability assessments.

Ground-based Midcourse Defense (GMD)

Executive Summary

- Previous assessments of the Ground-based Midcourse Defense (GMD) system remain unchanged. GMD has demonstrated a limited capability to defend the U.S. Homeland from small numbers of simple intermediate-range or intercontinental ballistic missile threats launched from North Korea or Iran. DOT&E cannot quantitatively assess GMD performance due to lack of ground tests supported by accredited modeling and simulation (M&S).
- The Missile Defense Agency (MDA) demonstrated Alternate Divert Thrusters (ADTs) for future Ground-Based Interceptors (GBIs) during the Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+) flight test. Extensive phenomenology data were also collected for discrimination improvement.
- The MDA executed the Ground Test, Integrated-06 (GTI-06) Part 2 and Ground Test, Distributed-06 (GTD-06) Part 2 ground tests assessing Ballistic Missile Defense System (BMDS)-level strategic and theater/regional capabilities in U.S. Northern Command's (USNORTHCOM's) and U.S. Pacific Command's (USPACOM's) areas of responsibility. The MDA demonstrated BMDS interoperability and updated discrimination capability. The lack of accreditation of models and simulation for performance assessment limited using these data for quantitative GMD evaluation.
- The MDA emplaced six GBIs with upgraded Capability Enhancement-II (CE-II) Exo-atmospheric Kill Vehicles (EKVs) and Configuration 1 boosters.
- The MDA declared the In-Flight Interceptor Communication System Data Terminal (IDT) at Fort Drum, New York, available and USNORTHCOM accepted the site in December 2015. USNORTHCOM opened the site for operational use in July 2016.

System

- GMD counters intermediate range and intercontinental ballistic missile threats to the U.S. Homeland. GMD consists of:
  - GBIs at Fort Greely, Alaska, and Vandenberg AFB, California
  - GMD ground system, including GMD Fire Control (GFC) nodes at Schriever AFB, Colorado, and Fort Greely, Alaska; Command Launch Equipment (CLE) at Vandenberg AFB, California, and Fort Greely, Alaska; and IDTs at Vandenberg AFB, California, Fort Greely, Alaska, and Eareckson Air Station, Alaska
  - GMD secure data and voice communications system, including long-haul communications using the Defense Satellite Communication System, commercial satellite communications, and fiber-optic cable (both terrestrial and submarine)
  - External interfaces that connect to Aegis Ballistic Missile Defense (BMD) ships; North American Aerospace Defense/USNORTHCOM Command Center; Command and Control, Battle Management, and Communications (C2BMC) system at Schriever AFB, Colorado, and Pearl Harbor-Hickman AFB, Hawaii; Space-Based Infrared System (SBIRS) at Buckley AFB, Colorado; and AN/ TPY 2 (Forward Based Mode (FBM)) radars at Japan Air Self Defense Force bases in Shariki and Kyoga-Misaki, Japan

Mission

Military operators from the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (the Army component to U.S. Strategic Command) will use the GMD system to defend the U.S. Homeland against intermediate range and intercontinental ballistic missile attacks using the GBI to defeat threat missiles during the midcourse segment of flight.

Major Contractors

- GMD Prime: The Boeing Company, Network and Space Systems – Huntsville, Alabama
- Boost Vehicle: Orbital ATK, Missile Defense Systems – Chandler, Arizona
- EKV: Raytheon Company, Missile Systems – Tucson, Arizona
- Fire Control and Communications: Northrop Grumman Corporation, Information Systems – Huntsville, Alabama

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA conducted a non-intercept GM CTV-02+ flight test in January 2016. The MDA designed this test to demonstrate ADTs for future GMD interceptors and collect data for use in developing discrimination improvements.
- The MDA executed the GTI-06 Part 2 and GTD-06 Part 2 ground tests in May and September 2016, respectively. The MDA assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's areas of responsibility in integrated (i.e., GTI) and distributed (i.e., GTD) test environments. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks. The MDA used hardware and software representations of the GMD system; SBIRS; Upgraded Early Warning Radars (UEWRs); C2BMC; an AN/TPY-2 (FBM) radar; an Aegis AN/SPY-1 radar in its long-range surveillance and track mode; and the Sea-Based X-band (SBX) radar. In these tests, the MDA exercised the new GFC software version 6B3.1.
- The MDA emplaced six GBIs with upgraded CE-II EKVs and Configuration 1 boosters.
- The MDA completed the Redesigned Kill Vehicle System Requirements Review in November 2015.
- The MDA declared the IDT at Fort Drum, New York, available for use and USNORTHCOM accepted the site in December 2015. USNORTHCOM opened the site for operational use in July 2016.

Assessment

- Previous assessments of GMD remain unchanged. GMD demonstrates a limited capability to defend the U.S. Homeland from small numbers of simple intermediate-range or intercontinental ballistic missile threats launched from North Korea or Iran.
  - The reliability and availability of the operational GBIs are low, and the MDA continues to discover new failure modes during testing.
  - GMD survivability data are limited and come primarily from facility testing and component-level testing, but known survivability issues exist. Few cybersecurity assessments have been performed to-date.
  - Radar availability shortfalls, the details of which are classified, affect GMD suitability.
- During GM CTV-02+, the MDA demonstrated the new CE-II EKV ADTs in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally. One controller circuit board associated with one of the ADTs experienced a short and did not command its ADT to turn on for the later part of the test. This controller circuit board is contained within the GBI guidance module and is not considered part of the ADT subsystem. An anomaly review board determined that foreign object damage was the most likely cause of the controller circuit board failure. The MDA collected extensive phenomenology data for discrimination improvement.
- In GTI-06 Part 2 and GTD-06 Part 2 ground tests, the MDA demonstrated interoperability of the GMD GFC software version 6B3.1 with the SBIRS, UEWRs, C2BMC, AN/TPY-2 (FBM) radar, Aegis BMD AN/SPY-1 radar in its long-range surveillance and track mode, and SBX radar. Discrimination improvements were ground tested as part of the BMDS Capability Increment 3 delivery. A number of GMD software upgrades were ground tested, including the discrimination logic, SBX tasking, and GFC salvo logic. These data support the evaluation of GMD system performance against an expanded strategic threat set.
- Quantitative evaluation of GMD performance will require extensive ground testing with accredited M&S. Data needed to accredit GMD threat, radar, and environmental M&S are either limited or lacking. GMD intercept flight tests have not adequately spanned the operational battlespace to provide data for validation, and subsequent accreditation, of key M&S.

Recommendations

- Status of Previous Recommendations. The MDA has completed previous recommendations with the exception of one FY14 and one FY15 recommendation:
  1. The MDA has initiated, but not completed, the FY14 recommendation to extend the principles and recommendations contained in the Independent Expert Panel assessment report on the GBI fleet to all Homeland Defense components of the BMDS.
  2. The MDA should determine any additional sensor capability requirements for an effective Defense of Hawaii capability (FY15 recommendation). The MDA has initiated analysis of the needed capability, but has not completed this study.
- FY16 Recommendations. The MDA should:
  1. Improve and demonstrate the reliability and availability of the operational GBIs.
  2. Increase emphasis on GMD survivability testing, including cybersecurity. Tests, demonstrations, and exercises to acquire additional survivability data should be planned for inclusion in the BMDS Integrated Master Test Plan.
  3. Accelerate its effort to accredit M&S for performance assessment supporting GMD OT&E, including Redesigned Kill Vehicle performance and lethality.

Terminal High-Altitude Area Defense (THAAD)

Executive Summary

- The Terminal High-Altitude Area Defense (THAAD) program participated in one Ballistic Missile Defense System (BMDS) operational flight test in November 2015, in accordance with the DOT&E-approved Integrated Master Test Plan, intercepting two ballistic missile targets.
- THAAD participated in four BMDS ground tests, providing information on THAAD interoperability and functionality within the BMDS for various regional/theater scenarios.
- The THAAD program conducted a Cybersecurity Red Team Assessment in March 2016 and a Limited User Test of the Table Top Trainer in June 2016.
- The THAAD program continued work on achieving a Full Materiel Release of the first two THAAD batteries, which achieved Conditional Materiel Release in February 2012.

System

- THAAD is intended to complement the lower-tier Patriot system and the upper-tier Aegis Ballistic Missile Defense (BMD); it can engage threat ballistic missiles in both the endo- and exo-atmosphere.
- THAAD consists of five major components:
  - Missiles
  - Launchers
  - AN/TPY-2 Radar (Terminal Mode)
  - THAAD Fire Control and Communications
  - THAAD Peculiar Support Equipment
- THAAD can accept target cues for acquisition from Aegis BMD, from other regional sensors, and through command and control systems.

Mission

U.S. Strategic Command deploys THAAD to protect critical assets worldwide. U.S. Northern Command, U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) will use THAAD to intercept short- to intermediate-range ballistic missile (SRBM/IRBM) threats in their areas of responsibility.

Major Contractors

- Prime: Lockheed Martin Corporation, Missiles and Fire Control – Dallas, Texas
- Interceptors: Lockheed Martin Corporation, Missiles and Fire Control – Troy, Alabama
- AN/TPY-2 Radar (Terminal Mode): Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts

Activity

- The Missile Defense Agency (MDA) conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA conducted system-level Flight Test Operational-02 (FTO-02) Event 2a in November 2015 at Wake Island and the broad ocean area surrounding it. This test used THAAD version 2.7 software and a Lot 4 and Fire Unit Fielded interceptor. THAAD completed near-simultaneous engagements of two targets: a complex SRBM and a medium-range ballistic missile (MRBM). The engagement of the MRBM occurred following the failure of an Aegis BMD Standard Missile-3 Block IB guided missile to intercept the target. An AN/TPY-2 (Forward-Based Mode) radar, in addition to the THAAD (Terminal Mode) radar, also tracked the targets. The MDA initially attempted to conduct this test in October 2015 as FTO-02 Event 2; however, due to a THAAD target malfunction, the event was a "No Test."
- THAAD provided hardware-in-the-loop representations for four BMDS ground tests that provided information on THAAD interoperability and functionality in various regional/theater scenarios.
  - Ground Test Distributed-06 (GTD-06) Part 1 in October 2015 examined defense of USEUCOM and USCENTCOM scenarios, using THAAD version 2.7 software.

- Ground Test Integrated-06 (GTI-06) Part 2 in April 2016 examined defense of USPACOM and Homeland defense scenarios, using THAAD version 2.8 software.
- GTI-Israel-16 in June 2016 studied interoperability between the BMDS and the Arrow Weapon System for maintaining shared situational awareness, using THAAD version 2.7 software.
- GTD-06 Part 2 in September 2016 again examined defense of USPACOM and Homeland defense scenarios, using THAAD version 2.8 software.

• The THAAD program also conducted several smaller test events including a Cybersecurity Red Team Assessment in March 2016 and a Limited User Test of the Table Top Trainer in June 2016.

Assessment

• FTO-02 Event 2a demonstrated that THAAD capabilities against theater and regional threats increased during FY16. THAAD Lot 4 and Fire Unit Fielded interceptors, for the first time, intercepted one complex SRBM and one MRBM threat-representative ballistic missile target while Aegis BMD simultaneously engaged an air-breathing threat. In addition to testing against new threat characteristics, the MDA successfully demonstrated the THAAD radar advanced algorithms for the first time during this test. The test event also demonstrated that recent obsolescence redesigns of hardware and software, which were fully integrated for the first time in this test, caused unintended problems. The THAAD Project Office should further study these design changes to minimize their negative effects.

• Although THAAD has been deployed to Guam since 2013, THAAD has not yet demonstrated capability against IRBM threats in a flight test. The MDA will demonstrate this capability in FY17 during Flight Test THAAD-18 (FTT-18). This test, in addition to previous flight testing and FTT-15 (also planned for FY17), will demonstrate several key capabilities against longer range threats that the MDA should further explore using end-to-end modeling and simulation.

• During GTD-06 Part 1, GTI-06 Part 2, and GTD-06 Part 2, the MDA demonstrated aspects of THAAD functionality in different theater scenarios. The BMDS Operational Test Agency (OTA) also reported several findings, consistent with findings from earlier ground tests that affect THAAD interoperability, track management, and radar functions.

• Although analysis is still ongoing, data from FTO-02 Event 2 and Event 2a indicate that overall reliability failure rates were higher than those observed during the FY15 Reliability Growth Test. The launcher, particularly its 3-kilowatt generator, continued to experience failures.

• Problems previously discovered during testing, if not corrected, could adversely affect THAAD effectiveness, suitability, or survivability. These problems, the details of which can be found in DOT&E's classified 2015 Assessment of the BMDS, include:
  - Training and documentation are still immature. Training courses and aids are still in development, and errors and omissions in the technical manuals continue to be found during testing.
  - Environmental testing revealed some deficiencies which have not been corrected.
  - Some specific aspects of discrimination and classification need improvement.
  - Testing revealed some survivability and cybersecurity shortfalls, which are still in the process of being fixed and assessed.

• The THAAD program continued work on achieving a Full Materiel Release of the first two THAAD batteries, which achieved Conditional Materiel Release in February 2012. The THAAD Project Office continued to address the 19 open conditions that need to be resolved before the Army will grant a Full Materiel Release. The THAAD program will continue to test and fix the open conditions through FY19. Of the original 39 conditions, the THAAD Project Office closed 20 conditions in FY12-15 and 1 condition to "provide a capability to electronically transfer battle plans" in FY16.

• Work also continues on additional materiel release conditions for follow-on THAAD software versions 1.3.1, 1.4.0, and 2.7.0 (Configuration 2).

Recommendations

• Status of Previous Recommendations. DOT&E's classified February 2012 THAAD and AN/TPY-2 Radar OT&E and LFT&E report contained 7 recommendations in addition to the 39 Conditional Materiel Release conditions. The MDA should continue to address the two remaining classified recommendations (Effectiveness #2 and Effectiveness #5) and the two remaining unclassified recommendations. The MDA and the Army should:
  1. Implement equipment redesigns and modifications identified during natural environment testing to prevent problems seen in testing (Suitability #11). Some of these deficiencies have been addressed by hardware modifications included in THAAD Configuration 2. Conducting additional ground testing with Configuration 2 (a standing FY14 recommendation) would also provide data to address this recommendation.
  2. Conduct electronic warfare testing and analysis (Survivability #3). The MDA conducted preliminary testing during FY13, but additional testing is required.
  3. The program partially addressed the FY14 recommendation to conduct thorough end-to-end testing of the THAAD Configuration 2 that incorporates considerable obsolescence redesigns of hardware and software. The MDA should continue to plan to rigorously ground test the THAAD system to verify that these changes can withstand the range of environments and conditions required.
  4. The program has begun to address the FY15 recommendation that the MDA should prioritize flight and ground testing that involves THAAD and Patriot engagement coordination, to determine if the information passed between THAAD and Patriot does not disrupt organic intercept capabilities and can contribute to reduced

interceptor wastage and threat missile leakage. The MDA and Army are considering a combined THAAD and Patriot test in 2018.

- FY16 Recommendation.
  1. The MDA and BMDS OTA should plan to conduct high-fidelity modeling and simulation runs against longer range threats following the FTT-18 and FTT-15 flight test campaign, to include endgame and lethality analyses for these tests.

Live Fire Test and Evaluation

Live Fire Test and Evaluation

Live Fire Test and Evaluation (LFT&E)

INTRODUCTION

- In FY16, DOT&E executed LFT&E oversight for 132 acquisition programs, 3 LFT&E investment programs (Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), Joint Aircraft Survivability Program (JASP), and Joint Live Fire (JLF)), and 3 special interest programs (Warrior Injury Assessment Manikin (WIAMan), Home Made Explosives (HME), and Small Boat Shooters' Working Group).
- In support of a range of acquisition decisions and activities, DOT&E published two LFT&E reports and two combined OT&E and LFT&E reports. The reports include recommendations to the Services to further improve the survivability or lethality of the subject systems for a range of operationally relevant scenarios in existing and expected combat environments.

LFT&E Investment Programs Summary

- The Joint Technical Coordinating Group for Munitions Effectiveness:
  - Enhanced the capabilities of its two major products – the Joint Munitions Effectiveness Manual (JMEM) Weaponeering System (JWS) and Joint-Anti-air Combat Effectiveness (J-ACE) – to meet new Combatant Commands' requirements. These efforts equipped the Combatant Commands with added operational targeting, weaponeering data and solutions, and collateral damage estimation capability in direct support of new operations, mission planning, and training. This includes the Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool and Digital Imagery Exploitation Engine (DIEE), as well as standalone resources such as the Probability of kill (Pk) Lookup Tools, Collateral Damage Estimation (CDE) tables, and munitions weaponeering guides. These solutions rapidly provide Service members with authoritative weapons effectiveness data when needed, as well as seamless end-to-end strike package development during planning (i.e., weaponeering, collateral damage estimation, and precision point mensuration).
  - Supported the air warfare community – in particular the Naval Strike and Air Warfare Center and the Air Force Weapons School – with its J-ACE tool to develop tactics, techniques, and procedures manuals for air superiority applications and to perform post-shot analysis following exercise and training missions (e.g., Red Flag FY16 exercises at Nellis Test and Training Range, Nellis AFB, Nevada).
  - Worked with DOD, Joint, and Service planners to support force-on-force modeling, mission area analysis, requirements studies, and weapon procurement planning such as the Army's Total Army Analysis, the Air Force's Nonnuclear Consumables Annual Analysis, the Navy's Naval Munitions Requirements Process assessment, and annual Army Capabilities Integration Center simulation exercises.
  - Supported the acquisition community in performance assessments, analysis of alternatives (AoA), and survivability enhancement studies such as the Army's Echelon Above Brigade M113 Family of Vehicles Replacement AoA. This AoA leveraged standard JTCG/ME analytical tools, such as the Joint Mean Area of Effectiveness Model.
  - Developed a preliminary non-kinetic JMEM capability, to include a prototype Cyber JMEM. This provided the analytical foundation for standard processes and data to enable effectiveness estimates for cyber, electronic attack, and directed energy capabilities.
  - Continued work on JWS versions releasable to the United Kingdom, Canada, Australia, Republic of Korea, and other coalition partners for planning, operational weaponeering and collateral damage estimates, support of training and tactics development, and support of force-level analyses.
- JASP funded 47 multi-year projects addressing aircraft survivability enhancement technologies and aircraft survivability evaluation tools. In FY16, JASP made progress in improving:
  - The ability of aircraft to counter near-peer and second-tier threat by 1) developing and testing countermeasure techniques, which included improving both the fidelity of countermeasure simulations and the collection of flight test data on a new chaff design; 2) updating survivability tools such as the Enhanced Surface-to-Air Missile Simulation (ESAMS) with the latest threat types and countermeasures; and 3) investigating new countermeasure concepts for emerging threats.
  - Aircraft force protection by 1) developing improved hostile fire detection; 2) investigating anti rocket-propelled grenade warhead concepts to improve rotorcraft survivability; 3) investigating aircraft hardening against high energy lasers; and 4) improving the accuracy and confidence of vulnerability assessment tools.
  - Aircraft survivability to fires, the primary threat-induced aircraft vulnerability.
- JLF supplemented LFT&E of fielded systems, addressed operational commander's needs, and characterized new survivability and lethality effects of fielded systems either: 1) in response to the exposure of U.S. systems to new threats; 2) as a result of systems being used in new, unanticipated

ways; or 3) as a result of systems being operated in new environments. Specifically, JLF:
- Assessed the effect of fielded system design changes on survivability (e.g., CV-22 add-on armor)
- Assessed weapon lethality of a new ammunition mix for A-10 aircraft as well as behind armor debris of an anti-tank penetrator mine
- Improved the accuracy and fidelity of weapon data used as part of mission planning in order to estimate weapon effectiveness and effects with higher confidence (e.g., improved collateral damage estimates)
- Advanced live fire test methodology to improve collection of fragment velocity and spatial distribution data during arena testing
- Supported the development and improvement of modeling and simulation tools that contribute to survivability and lethality evaluations (e.g., new data to support improvements in predicting weapons effects against aircraft, vehicles, and military structures)

LFT&E Special Interest Programs Summary

- The WIAMan project, an Army-led effort, made significant progress in biomechanics testing and anthropomorphic test device development to design a biofidelic prototype for assessing injuries to vehicle occupants during underbody blast. However, the Army has not programmed the funding for this project in FY18 or beyond, which could adversely affect the delivery of this capability.
- HME-C investigated and tested the repeatability of HME surrogate effects relative to those of TNT and the effects of soil condition and IED emplacement on HME threat performance. DOT&E used the test data to develop LFT&E policy for employing buried underbody blast surrogates that mitigates soil-induced test data variability. This included a new, engineered soil standard for use with underbody blast testing.
- The Small Boat Shooters' Working Group continues to synchronize live fire and other operational test approaches against this growing threat class, which operates in littoral waters.
- DOT&E briefed Congressional staff on helicopter seating system improvements per the House Report to accompany the National Defense Authorization Act for FY16. DOT&E determined that seating system improvements would improve force protection in some crash conditions, but addressing controlled flight into terrain and collision threat avoidance with near-term technology solutions would provide a higher payoff by mitigating leading cause of fatality in helicopter mishap and combat-induced crashes.

LFT&E ACQUISITION PROGRAMS

- The primary objective of LFT&E is to evaluate the survivability and lethality of acquisition programs and to identify system design deficiencies to be corrected before those platforms or munitions get deployed or enter full-rate production. In FY16, DOT&E executed LFT&E oversight for 132 acquisition programs. Of those, 17 operated under the waiver provision of U.S. Code, Title 10, Section 2366, by executing an approved alternative LFT&E strategy in lieu of full-up system-level testing. DOT&E published two LFT&E reports and two combined OT&E and LFT&E reports in FY16 (see Table 1).

LFT&E Reports	Combined OT&E and LFT&E Reports
Multiple Launch Rocket System (MLRS) M270A1 Launcher Improved Armored Cab (IAC)*	Mine Resistant Ambush Protected (MRAP) Family of Vehicles MaxxPro Long Wheel Base (LWB) Ambulance with Independent Suspension System (ISS) and MaxxPro Survivability Upgrade
Soldier Protection System (SPS) Torso and Extremities Protection (TEP)*	M829A4 120 mm Armor-Piercing, Fin Stabilized, Discarding Sabot – Tracer (APFSDS T)*

* Reports sent to Congress.

- Three reports supported Full-Rate Production decisions:
  - "Multiple Launch Rocket System (MLRS) M270A1 Launcher Improved Armored Cab (IAC)" reported on the protection that the IAC provides to the MLRS crew. The report included three recommendations to improve MLRS crew survivability.
  - "Soldier Protection System (SPS) Torso and Extremities Protection (TEP)," regarding a single soft armor system to replace the Army's Improved Outer Tactical Vest, reported on the protection the TEP provides soldiers against small-arms and fragmenting threats.
  - "M829A4 120 mm Armor-Piercing, Fin Stabilized, Discarding Sabot – Tracer (APFSDS-T)" reported on the lethality of the M829A4 120 mm APFSDS-T. This report included four recommendations to improve operational effectiveness and lethality, and one recommendation to improve test and evaluation practices in future similar lethality test programs. DOT&E continues to observe the follow-on tests and will report on the accuracy problems with the M829A4 service rounds that were observed during the User Beta Test for Version 4.6 of the Abrams software.
- One report provided a system survivability evaluation for use by the Service and Program Office:
  - "Mine Resistant Ambush Protected (MRAP) Family of Vehicles MaxxPro Long Wheel Base (LWB) Ambulance

with Independent Suspension System (ISS) and MaxxPro Survivability Upgrade" reported on the protection against underbody blasts afforded to occupants of the MaxxPro LWB Ambulance MRAP vehicle (also known as the M1266A1). LFT&E made five recommendations to further reduce the underbody vulnerability of the M1266A1 and its crew.

- DOT&E published one classified Special Report, "Market Survey of Active Protection Systems," in response to Senate Committee Report 114-49 (2015).
- DOT&E provided the classified "Assessment of the Performance and Effectiveness Characteristics of the 5.56 mm M855A1 and Mk318 Mod 1 Rounds" to the Under Secretary of Defense for Acquisition, Technology and Logistics in response to Senate Committee Report 114-49 (2015).

LFT&E INVESTMENT PROGRAMS

JOINT TECHNICAL COORDINATING GROUP FOR MUNITIONS EFFECTIVENESS

The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) continued to update and develop weapons effectiveness and target vulnerability data, standards, and methodologies that are crucial for developing theater commanders' force employment options as well as the resulting execution tasking orders to tactical units. The principal products of the JTCG/ME are the Joint Munitions Effectiveness Manuals (JMEMs). JMEMs enable users to plan the mission adequately by determining the effectiveness of weapon systems against a specified target for a range of weapon delivery modes. JMEMs include: detailed data on the physical characteristics and performance of weapons and weapon systems; descriptions of the mathematical methodologies that employ these data to generate effectiveness estimates; software that permits users to calculate effectiveness estimates; and pre-calculated weapon effectiveness estimates. This information enables a standardized comparison of weapon effectiveness across all Service communities. JMEM products include existing software product lines, such as the JMEM Weaponeering System (JWS) and the Joint Anti-air Combat Effectiveness. Future product lines will include the Joint Non-Kinetic Effectiveness capability. Specialized solutions are driven by the needs of Combatant Commands and lessons learned from current operations. Such solutions include Probability of kill (Pk) Lookup Tools; Collateral Damage Estimation (CDE) tables; munitions weaponeering guides; and enablers for more efficient targeteering (e.g., the Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool and the Digital Imagery Exploitation Engine (DIEE)).

Joint Munitions Effectiveness Manual Weaponeering System

- JWS is the DOD source for air-to-surface and surface-to-surface weaponeering, munitions, and target information used daily by the U.S. Central Command (USCENTCOM), U.S. Special Operations Command (USSOCOM), and U.S. Africa Command (USAFRICOM) in the deliberate planning process directly supporting Joint Publication 3-60, "Joint Targeting."
- JWS enables Combatant Commands to prosecute their target sets. JWS incorporates accredited methodologies, certified munition characteristics, delivery accuracy, target vulnerability data, and numerous user aids to support the operational use of JWS to predict weapons effectiveness for fielded weapons and delivery systems.
- JTCG/ME deployed JWS v2.2 in FY16. JWS v2.2 included a total of 220 methodology, functionality, weapons/warheads/fuzes, and target updates. JWS v2.2 included initial connectivity with the DCiDE tool (Figure 1), as well as updates to the Fast Integrated Structural Tool (FIST) (containing building types and a quasi-static blast capability). The connectivity with DCiDE improves both speed and throughput of data.
- JTCG/ME continued to facilitate coalition interoperability. It is currently completing several JWS version releases to key coalition partners in support of current operations under Foreign Military Sales agreements. This capability improves the effectiveness of U.S. fires and targeting personnel working in combined environments.
- JTCG/ME continued development on JWS v2.3 in FY16; fielding is scheduled in 1QFY17. JWS v2.3 will include enhanced data sets and capabilities with a focus on connectivity to other targeting and mission planning capabilities for improved estimates and more seamless planning. More specifically, JWS v2.3 enhanced capabilities include:
  - Connectivity to the Modernized Integrated Database, Joint Targeting Toolbox, and DIEE (currently in finalization for separate fielding). This will permit automatic transfer of data and information between these planning tools.
  - Multiple updates to FIST to incorporate connectivity with DIEE and the Joint Targeting Toolbox, along with updated target options (such as building type, material, and features). These updates will improve weapons effectiveness estimates.
  - Improvements to the Ship Weaponeering Estimation Tool that optimize database use and improve the user interface.
  - Inclusion of a weapon delivery accuracy module along with updates for the Gunship Delivery Accuracy Program, Rotary Wing Delivery Accuracy Program, and Joint Delivery Accuracy Program. This will provide enhanced calculations for F-35 gun munitions and C-130 gunship effectiveness in JWS.

- The Dilution of Precision Tool, which improves the predicted accuracy of GPS/Inertial Navigation System weapons from satellite time and space calculations.
- The Target Location Error Tool, which enables a single JWS tool to provide Target Location Error from airborne and ground based sensors.
- Updates on weapons delivery accuracy and characterization data for multiple systems (e.g. M982 Excalibur satellite-guided artillery shell, M395 Precision Guided Mortar Munition, AGM-65E2/L Maverick air-to-ground tactical missile, M1061 60 millimeter mortar, M120 Towed/M121 120 millimeter mortar, BLU-110 general purpose bomb, AGM-114 Hellfire variant, M31 Guided Multiple Launch Rocket System, M1156 Precision Guidance Kit, and numerous small arms).
- Fifty target vulnerability data sets across ground, aircraft, small boats, ships, and submarines, as well as 352 updated image Quickfacts, which provide the Weaponeer quick-reference characteristics of systems for analysis.

• JTCG/ME will continue development of JWS v2.4 during FY17 to provide enhanced data capabilities and connectivity.

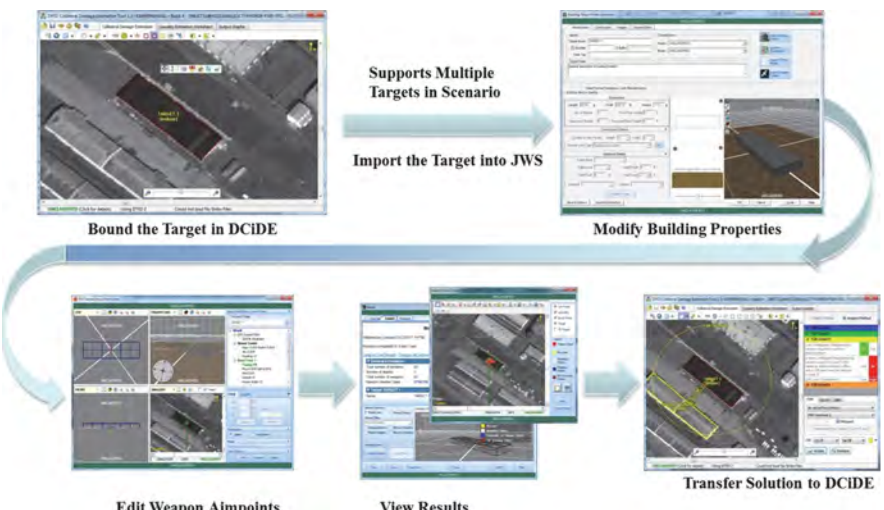


Figure 1. Connectivity between Weaponeering and Collateral Damage Assessment Enables Combatant Commanders to More Rapidly Prosecute Targets

In FY16, JTCG/ME released DCiDE v2.0 to support the Chairman of the Joint Chiefs of Staff Instruction 3160.01B, "No-Strike and the Collateral Damage Estimation (CDE) Methodology." This release provides the latest approved Collateral Effect Radii (CER) and CDE data as of FY16.

- The DCiDE tool is an accredited and automated CDE tool that expedites and simplifies the CDE process. As such, it is critical to the Warfighters' ability to meet urgent operational needs. DCiDE is the only automated CDE tool authorized for use in the USCENTCOM and USAFRICOM Areas of Responsibility Operation (AORs). The JTCG/ME CDE tables are used in every planned kinetic strike in all AORs to meet Commanders' intent and to minimize civilian casualties. DOT&E continues to receive positive feedback on the use of the CER values, collected as part of the Joint Live Fire efforts, as a critical enabler in support of munitions employment against HVTs.
- JTCG/ME updated the accredited CER Reference Tables for selected air-to-surface and surface-to-surface weapons, which are the basic data that support the CDE methodology. Changes included additions for airburst munitions, nomenclature changes, and additional updates for newly fielded/updated systems (e.g., HELLFIRE family). JTCG/ME also developed and accredited the Collateral Effects Library tool in support of advanced CDE mitigation techniques.

• JTCG/ME is working with the Navy's DPSS program based at the Naval Air Weapons Center – Weapons Division in China Lake, California, to provide the Digital Imagery Exploitation Engine (DIEE). DIEE is an enterprise targeting solution that provides both seamless planning with the various planning tools and a direct linkage to mission planning systems in operational units.
  - DIEE is a self-contained Government off-the-shelf (GOTS) computer system with internal software. It can derive mensurated coordinates from the Digital Point Positioning Database and will combine applications so that targeting or planning personnel can develop strike plans where the weaponeering, collateral damage estimation, and precision point mensuration conducted during planning is both seamless and linked to mission planning systems for target execution. JTCG/ME began fielding DIEE at the beginning of FY17, and both USCENTCOM and USARFICOM have already committed to using DIEE as their primary targeting planning tool.

Joint-Anti-air Combat Effectiveness

• Joint-Anti-air Combat Effectiveness (J-ACE) provides authoritative air-to-air and surface-to-air weapons effectiveness information, and serves as the primary tool used by the Air Force and Navy to underpin air combat tactics, technics, and procedures development. J-ACE is the umbrella program that includes both the Joint Anti-air Model (JAAM) and Endgame Manager, which provides a full kill chain end-to-end capability. Other users include National Test and Training Ranges for air to air and surface to air shot validation and various members of the analytical community for air combat studies and planning. The U.S. Strategic Command (USSTRATCOM) leverages J-ACE capabilities to support route planning for the execution of strike packages. JAAM supports operational squadrons' mission debrief tools, such as the Personal Computer Debriefing System and several others.

• JTCG/ME is releasing J-ACE v5.3, which will extend and update data sets for missile and aircraft target aero performance, anti-air missile lethality, and air target vulnerability. These data include over 40 air-to-air missile models (blue and threat), over 50 surface-to-air missile models (threat), and approximately 40 aircraft models (blue and threat). New capabilities include:

  - The Hybrid Integration and Visualization Engine computer architecture interface
  - The BLUEMAX6 (six degrees of freedom aero performance) model for increased aircraft aero performance modeling, with Hands-on Throttle and Stick allowing for actual flight control of the aircraft
  - Increased countermeasure capabilities leveraging ESAMS
  - Factoring in the effect of weapon system reliability when calculating the probability of a successful engagement
  - The ability to estimate countermeasure effectiveness
- J-ACE v5.4 is in development to field and add Browse descriptive material to support new weapons in the JAAM and Endgame Manager. The fielding of J-ACE v5.4 in 2017 will facilitate greater connectivity for outbrief capability by units, target detection estimation, counter air defense prediction capability, and enhanced architecture allowing future version growth and compatibility.

Joint Non-Kinetic Effectiveness – Cyber/Electronic Attack and Directed Energy JMEMs

- JTCG/ME is continuing the development of non-kinetic weaponeering tools and methodologies. Joint Non Kinetic Effectiveness is intended to be the single source for operational Warfighters, analysts, targeteers, and planners to analyze offensive cyber capabilities, electronic attack weapons, and directed energy effectiveness.
- In conjunction with DOT&E and the Air Force's 363rd Intelligence, Surveillance, and Reconnaissance Group, the JTCG/ME continued development of a JMEM process for cyberspace operations, electronic attack, and directed energy. FY16 efforts centered on developing the foundational elements for JMEM production, including weapons characteristics, target vulnerability, and effects estimation tools (e.g., U.S. Cyber Command's Cyber Capabilities Registry, Electronic Warfare/Cyber Critical Elements/Weaponeering Guides, and Directed Energy Effectiveness Lookup Tables). These efforts culminated in an initial Cyber JMEM prototype for user review and set the foundation for a full joint non-kinetic suite that includes other non-kinetic effects.

Operational Users Working Group

- The Operational Users Working Group is a critical venue for receiving direct user feedback and development of future requirements from the operational community in regards to needed software enhancements and capabilities to support air-to-surface, surface-to-surface, anti-air, and non-kinetic engagements. Examples of user requirements include the ability to release weaponeering information to coalition partners; connectivity between tools and mission planning systems; current weapon and fuze information; updated training materials; quick weaponeering guides; graphical user interface enhancements; and improved blast/fragment methodologies in support of small precision munitions.
- JTCG/ME continued to chair Operational Users Working Groups with representatives from USCENTCOM, USAFRICOM, USSTRATCOM, U.S. Pacific Command, USSOCOM, the Services, the Defense Intelligence Agency, the Defense Threat Reduction Agency, the Fires Center of Excellence, Service School Houses, the Marine Aviation Weapons/Tactics Squadron, Operations Support Squadrons, Intelligence Squadrons, and numerous operational units.

Joint Aircraft Survivability Program

The mission of the Joint Aircraft Survivability Program (JASP) is to increase military aircraft combat survivability – and, by extension, effectiveness – in current and emerging threat environments. JASP supports the mission through funding and oversight of Research, Development, Test, and Evaluation to develop aircraft survivability technologies and assessment methodologies. JASP also supports the mission through cross-Service coordination, educating the community about aircraft survivability, maintaining and improving core survivability tools, and taking a lead role in combat data collection. In FY16, JASP funded 47 multi-year projects and delivered 27 final reports. In FY16, JASP focused on projects intended to either 1) defeat near-peer and second-tier adversary threats by developing measures to avoid detection and counter engagement of advanced radio frequency and infrared guided threats; 2) improve aircraft force protection; or 3) improve aircraft survivability to combat-induced fires.

Defeat Near-Peer and second-Tier Adversary Threats

To defeat near-peer and second-tier adversary threats, JASP focused on developing: 1) measures to counter adversary radio frequency-guided threats and anti-access/area-denial capabilities, coupled with quantifiable improvements in ESAMS and Hardware-in-the-Loop capabilities; and 2) measures to counter emerging infrared homing threats with advanced counter-countermeasures, coupled with quantifiable improvements in The Modeling System for Advanced Investigation of Countermeasures (MOSAIC) and Hardware-in-the-Loop capabilities.

- ESAMS is the primary tool used by Government and Industry to assess the engagement of U.S. aircraft by radar-directed surface-to-air missile systems. JASP, in coordination with the Air Force Life Cycle Management Center, developed several upgrades to ESAMS to maintain its relevancy to current and future threat environments. These upgrades include:
  - The capability to model the flow fields around chaff release to more accurately represent chaff bundle dispersion patterns. This capability will be released in ESAMS v5.3 in March 2017.
  - Integration of an advanced naval surface-to-air missile threat, which was developed in cooperation with the Office of Naval Intelligence. This capability will be released in ESAMS v5.3 in March 2017.
  - Improvement of two threat engagement radar models by adding their electronic counter-countermeasure capabilities. These upgrades will be released in ESAMS v5.4 in FY18.
- MOSAIC is the primary digital tool used to develop and assess effective U.S. aircraft infrared countermeasures (IRCM).

- JASP concluded a multi-year effort with Large Aircraft IRCM (LAIRCM) and Common IRCM (CIRCM) program support elements of the Air Force Research Laboratory and the Naval Surface Warfare Center, Crane Division to verify and validate MOSAIC for LAIRCM IOT&E. This effort verified and validated nine threat missile models in MOSAIC for directed energy IRCM supporting LAIRCM, CIRCM, and other future system development, test, and evaluation.

- A continuing need across the DOD is ready access to valid countermeasure characterization model data. The ability to model countermeasures is a critical component in the threat engagement simulations used to develop and optimize tactics, techniques, and procedures (TTPs) in response to near-peer and second-tier adversary threat improvements.
  - JASP funded the Army's Armament Research, Development and Engineering Center in conjunction with Naval Air Systems Command (NAVAIR) to conduct flight tests to collect Radar Cross Section data on a new chaff design. The data will be used to determine the optimum response range of metamaterial for countering radio frequency threats. Initial analysis indicates that the chaff can be utilized from the S through W bands.
  - JASP funded the development of a physics-based model of chaff dispensed in airflow around fixed and rotary wing aircraft. This will improve modeling of the effectiveness of chaff as a countermeasure; current models do not optimize chaff dispersion based on the influences of aircraft flow field vortices. Additionally, chaff models estimate cloud growth based on empirical test data rather than physics-based modeling of individual particles on the Radar Cross Section or Doppler effects. NAVAIR conducted flight testing to collect chaff dispense characteristics in various fixed and rotary-wing aircraft flow fields. NAVAIR, the Army Aeroflightdynamics Directorate, and the Office of Naval Intelligence are working together to develop the Computational Fluid Dynamics model to include flow field effects.
- Helicopter loss rates during Operation Iraqi Freedom, Operation Enduring Freedom, and subsequent counterinsurgency operations were significantly reduced by employment of Missile Warning Systems and effective countermeasures. JASP funded the following efforts to develop technologies and techniques to counter newer classes of infrared-guided seekers:
  - Naval Research Laboratory development of missile warning algorithms using two-color infrared imagery for early identification of threat missiles to enhance countermeasure effectiveness. The main goals are to develop missile identification algorithms capable of exploiting two-color infrared imagery, determine the ability to perform missile identification in urban clutter, and characterize jamming performance for Distributed Aperture IRCM (DAIRCM).
  - Testing threat system Infrared Counter-countermeasures' performance against current countermeasure technologies using a two-color tracker to understand how color ratio is used to discriminate between flares and the target; the results will be used to develop more effective countermeasures.
  - Development of a new capability to field test missile seekers against model aircraft with countermeasures including paints and directed energy to optimize electro-optical/infrared countermeasures. The countermeasure effectiveness of various aircraft paints and paint schemes is determined by testing with a surrogate threat infrared seeker. The scale model test facility at the Naval Research Laboratory's Blossom Point Research Facility is a bridge in test capability between laboratory tests and field tests with full scale aircraft. Validation of seeker results provides a surrogate advanced threat seeker for use in countermeasure development and evaluation.
  - Investigation of the feasibility of using Ultra-Short Pulse lasers for aircraft IRCM. The results of the study will support an Office of Naval Research initiative to further test and develop Ultra-Short Pulse IRCM.
  - Completed design and testing of a standardized test set to measure expendable countermeasure launch setback forces. Developed a standard operating procedure to generate expendable countermeasure setback force data and created a database for tri-Service use. Standardizing the testing of expendable launchers (i.e., flare buckets) across the tri-Service community will minimize test duplication and reduce development costs.

Improve Aircraft Force Protection

To improve the ability of U.S. aircraft to avoid threat detection and to mitigate damage when hit, JASP funded several projects focused on the following objectives: improve situational awareness; counter unguided threats; harden aircraft systems; and improve the accuracy and confidence of vulnerability assessments.

- Improve Situational Awareness. JASP funded the Naval Research Laboratory to develop a sensor package that incorporates both mid-wave infrared (MWIR) and acoustic waveforms for detecting hostile fires and determining the location of the shooter. In FY16 (the second year of a three year program), the project enhanced the baseline approach to further reduce false alarms and improve shock wave propagation predictions. Shock-wave generation propagation simulation models and detection algorithm updates were provided to the DAIRCM program. The algorithm update achieved a 2.5X detection improvement in forward flight/maneuver and a greater than 10 percent improvement in hover over previous algorithms. Analysis of hostile fire detection system noise and performance on HH-60 corrected detection issues in forward flight maneuver.
- Counter Unguided Threats. Aircraft and crew losses to rocket-propelled grenades (RPGs) and other unguided threats are a concern for rotary-wing aircraft. JASP funded NAVAIR and the Army Armament Research, Development and Engineering Center (ARDEC) to develop an anti-RPG warhead. ARDEC

and NAVAIR developed four anti-RPG warhead concepts that could launch from a helicopter expendable countermeasure launcher. Testing of prototypes will begin testing in FY17, and the results will aid the Navy's Helicopter Active RPG Protection program.

- Harden Aircraft Systems. In FY16, JASP vulnerability reduction efforts focused on three major areas to improve aircraft force protection: RPG defeat, innovative opaque and transparent armors, and aircraft hardening against high-energy lasers (HEL). During FY16, JASP:
  - Determined, by compiling existing test data, that there is insufficient data on the response of the PG-7 piezo fuze to high-velocity impacts of common aircraft materials at oblique angles to model potential defeat mechanisms. Since RPG-7 testing has primarily focused on heavy track and ground vehicles there is little data to define constraints in designing solutions to mitigate RPG effects on aircraft.
  - Integrated low-power laser mitigation technology into the highly successful Multi Impact Transparent Armor System. For this initial JASP HEL hardening effort, the focus was to mitigate dazzling from a common, commercially available Nd:YAG (neodymium-doped yttrium aluminum garnet) laser at a wavelength of 1,064 nm. The technology blocked the targeted wavelength while maintaining a 97.2 percent transmission rate in the visible spectrum compared to the pre-notched baseline system with minimal transmission effect in the night vision goggle performance band. However, the system multi-hit capability was compromised due to the ceramic strike face de-bonding on the first hit. Additional development and testing is required before fielding.
  - Initiated a project to determine composite material loss of strength (under mechanical load) as a function of time when exposed to short-duration, high-intensity, thermal loads typical of HEL impingement. From this data, time-dependent probabilities of component damage (Pcd/h) curves can be developed for use in system-level vulnerability assessments.
- Improve the Accuracy and Confidence of Vulnerability Assessments. In FY16, JASP funded efforts to improve the accuracy and confidence of the prediction of projectile and warhead fragment penetration used to assess aircraft vulnerability.
  - JASP developed, implemented, and verified standard formats for the 11 threat projectiles and the 12 single fragments that are most often used in system-level aircraft vulnerability assessments and fire prediction studies. These files will provide consistency across studies performed by different organizations and will be incorporated into the unified threat characterization database that was released in the Air Force Vulnerability Toolkit v6.8 in December 2016.
  - JASP continued to improve projectile penetration predictions by converting the ProjPen projectile penetration model to a six degrees of freedom model with the goal of predicting residual yaw within five degrees and reducing the error in the prediction of system-level vulnerable area.

Improve Aircraft Survivability to Combat-Induced Fire.
Threat-induced fire is the largest potential contributor to fixed-wing aircraft vulnerability and the greatest source of uncertainty in aircraft vulnerability analysis. In FY16, JASP focused on developing solutions to maximize residual flight capability in the event of threat-induced onboard fires.

- JASP compiled and began evaluating data from across the Services to determine if self-sealing fuel bladders are performing as expected and whether military-standard qualification test methods adequately address threshold survivability requirements. JASP presented the results at the Tri-Service Fuel Bladder Roundtable and will document them in a final report.
- Developed and optimized, with a statistical design of experiments, next-generation self-sealing fuel bladder materials and construction layups. The next-generation bladders are lighter, more responsive to alternative aviation fuels and blends, and better at preventing fuel loss. Testing will continue during FY17.
- JASP continued work to optimize fire-resistant resin formulations for use as barrier ply on polymer matrix composites used in military aircraft. Integration of this type of resin could increase protection against internal fires and HELs. Coupon testing against heat flux conditions representative of small dry bay fires and HEL radiation is underway.

Combat Damage Assessment

- JASP enforced aircraft combat damage incident reporting in the Services and the DOD by continuing to support the Joint Combat Assessment Team (JCAT). The JCAT is a team of Army, Navy, and Air Force personnel that deploy to investigate aircraft combat damage in support of combat operations. JCAT ended its operation in Afghanistan in October 2014 with the return of deployed assessors to the United States. The team has continued to support assessments remotely from the continental United States and is ready to deploy rapidly outside of the United States if necessary.
- The JCAT started working with the U.S. Army Aeromedical Research Laboratory (USAARL) to study and document aviation combat injuries in Operation Iraqi Freedom and Operation Enduring Freedom. The results will be documented in USAARL reports and the Combat Damage Incident Reporting System.
- The JCAT and JASP program office worked in coordination with the Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Office of the Under Secretary of Defense for Personnel and Readiness, and the Joint Staff's Force Structure, Resource, and Assessment Directorate, J8, on an Aircraft Combat Damage Reporting (ACDR) Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P) Change Request (DCR) proposal that would institutionalize ACDR through changes in joint doctrine, training, information technology infrastructure, and policy. The DCR completed the Joint Staff review and comment process and was submitted for Joint Requirements Oversight Council approval.

- The JCAT trained the U.S. aviation community on potential aircraft threats and combat damage. This training includes but is not limited to: capabilities briefs, intelligence updates, recent "shoot-down" briefs to discuss enemy TTPs, and the combat damage collection and reporting mentioned above. The attendees include aircrews, maintenance personnel, intelligence sections, Service leaders, symposia attendees, and coalition partners.

The Joint Live Fire Program

In FY16, Joint Live Fire (JLF) funded 27 projects and delivered 21 reports. Focus areas for JLF included projects that either 1) characterized new survivability issues; 2) characterized new lethality issues; 3) improved accuracy and fidelity of weapon data; 4) improved test methods; or 5) improved modeling and simulation methods.

Characterization of New Survivability Issues

- Military Combat Eye Protection (MCEP) systems (spectacles, goggles) help protect soldier's eyes from debris and fragments associated with explosive munitions and IEDs. MCEP systems typically use lenses made from polycarbonate. JLF is assessing whether another material, Trogamid CX, is also a suitable lens material. Limited prior ballistic testing indicates Trogamid CX has superior ballistic impact resistance at room temperature.
  - JLF conducted testing to assess the ballistic performance of polycarbonate and Trogamid at various temperatures and to compare and contrast the ballistic performance of both materials.
  - The test data were used to develop curves that illustrate ballistic performance versus temperature for polycarbonate and Trogamid lenses, enabling a comparative assessment of the ballistic performance.
  - The data are currently being evaluated. The U.S. Army Natick Soldier Research, Development, and Engineering Center will use the results to assess the suitability of using Trogamid to manufacture protective eyewear in the future.
- Crew survivability in the event of a propellant fire onboard a M109A7 155 mm self-propelled howitzer is a concern. Unlike a fuel fire, a propellant fire is self-oxidizing and cannot be extinguished by the integral automatic fire extinguisher system; it has the potential to be more lethal to crewmen than a fuel fire.
  - JLF conducted a fire test focusing on the adequacy of various design solutions to improve crew survivability from a propellant fire prior to M109A7 full-rate production.
  - The data obtained during this test have been analyzed and will provide a basis for recommendations to improve M109A7 crew survivability. The recommendations will be included in the Live Fire Test and Evaluation Report provided as input to the March 2017 M109A7 full-rate production decision review.
- The U.S. military operates the C-12 aircraft in a number of roles including intelligence, surveillance, and reconnaissance; medical evacuation; and passenger and light cargo transport for the Army, Navy, Air Force, and Marine Corps in both hostile and non-hostile environments. However, the survivability of the C-12 aircraft in hostile environments has not been fully characterized. In FY16, JLF assessed the survivability of the C-12 due to direct ballistic engagements to the aircraft fuel system.
  - The results of this project will provide the information necessary to make informed operational and acquisition decisions based on an understanding of the likelihood and resulting damage levels from small arms threat engagements.
  - Since the fuel system is one of the largest contributors to aircraft ballistic vulnerability, this project examined ullage reaction to a variety of ballistic engagements. Data analysis is ongoing.
- JLF investigated the effectiveness of an improved ballistic armor system to protect CV-22 Osprey crewmembers from ballistic threats. The project used threats not previously tested as part of LFT&E to investigate the armor system performance when challenged along different shotlines. The results of this project will help guide future development efforts for the Osprey's next generation ballistic protection systems.
- Emerging High Energy Lasers (HELs) represent an emerging threat to aircraft and unmanned aerial vehicles (UAVs). The fuel systems of many UAVs have a large presented area which makes them vulnerable to HEL engagements. JLF obtained baseline damage-effects data for both fuel-backed dry bay and adjacent subsystems subjected to HEL thermal flux, and assessed both suppression of laser-induced dry bay fires and laser hardening methods. JLF will use the data to support modeling and simulation of HEL engagements and the improvement of hardening methods to reduce vulnerabilities from HEL engagements.

Characterization of New Lethality Issues

- JLF funded the Army Research Laboratory to characterize the behind armor debris (BAD) of an anti-tank penetrator mine. BAD consists of fragmentation from both the target vehicle's armor and the residual penetrator that spreads out as it is ejected into the vehicle's interior.
  - The additional BAD data for this threat will provide empirical data to support the design of protection systems against this threat.
  - The Army Research Laboratory will also use the test results to construct BAD models for use in vulnerability/lethality analyses. The Army Research Laboratory uses these BAD vulnerability/lethality analyses to support acquisition programs and the planning and evaluation of vehicle vulnerability testing.
- JLF funded the Air Force's 780th Test Squadron (780 TS) to conduct a modeling and simulation analysis to evaluate the lethality of a mix of 30 mm target practice ammunition and high-explosive incendiary (HEI) ammunition to determine the most effective alternative for the A-10's current combat mix.
  - The original A-10 combat load included a mix of both armor-piercing incendiary ammunition with depleted uranium penetrators and HEI ammunition. Environmental

health concerns with depleted uranium and aging-related reliability concerns have resulted in commanders using only HEI ammunition instead. This use of 100 percent HEI ammunition has demonstrated reduced lethality and effectiveness in engagements with combatants shielded by light armor vehicles, soft-skinned vehicles, or structures such as adobe brick walls.
  - This project has the potential to introduce an Urban Combat effective Mix (UCM) using target practice and HEI ammunition that provides an increased lethality over a 100 percent HEI combat load. Lessons learned from this application of target practice ammunition could later be applied to 20 mm and 25 mm weapon platforms for all users throughout the DOD. The results of this effort will also provide the Joint Munition Effectiveness Manual with 30 mm target practice round lethality data.
  - Live ammunition testing will occur in FY17 following the results of this modeling and simulation analysis.

Weapons Data Accuracy

- JLF was resourced to obtain new arena test data on the MK 84 general purpose bomb (Figure 2) due to concerns about the quality of existing MK 84 characterization data. JTCG/ME will incorporate the results of this test into JTCG/ME products. This testing complements similar testing done in FY15.
  - Initial examination of the fragment speeds from the test indicated a variance from the current characterization data. This variance has a strong potential to influence weapon usage for lethality, collateral damage estimates, and risk assessment.
  - In addition to the direct application of the characterization by the warfighter, JTCG/ME will compare the data with the output of shock physics predictive tools to improve the warhead detonation model in order to produce high fidelity results, potentially reduce the number of tests required for characterization of other warheads, and provide a better understanding of the fragment cloud.
  - Sandia National Laboratories utilized the test to explore optical fragment tracking techniques. These tracking techniques have the potential to provide additional data that will improve physics-based modeling.

Figure 2. Still photograph from MK 84 vertical arena test

- Mk 82 and Hellfire vs Adobe Walls. JLF funded the Naval Surface Warfare Center, Dahlgren Division to evaluate the effects of the blast and fragmentation from a MK 82 MOD 1 General Purpose bomb and HELLFIRE R9E warhead on adobe block structures.
  - JLF will collect critical data to determine a threshold radius for wall destruction.
  - The results will be used to improve collateral damage estimates and safe engagement distances for targets in close proximity to adobe buildings with civilian occupants. There currently exists no test data to support these estimates.
- Building Debris Characterization. JLF funded the Naval Surface Warfare Center, Dahlgren Division to conduct a test to characterize the secondary debris produced by detonation of a 105 mm PGU-44/B high-explosive projectile within a concrete masonry unit structure target (Figure 3).
  - JLF will collect critical information to characterize building debris in a manner similar to that of warhead fragments.
  - The results will be used to improve risk estimates of personnel injury resulting from both weapon fragments and building debris. No test data exists to support these estimates.

Figure 3. Concrete masonry unit for characterizing building debris

Improvements of Live Fire Test Methods

- Penetration Profiles of Ballistic Backing Material. JLF is investigating a test procedure to improve the characterization testing of materials currently being evaluated for use as backing material during ballistic testing of Personal Protective Equipment. The current clay backing material is subject to variations that can influence test results.
  - The current characterization tests for backing materials do not replicate the dynamic deformation rates those materials experience during ballistic testing.
  - The results of this effort will permit selection of backing materials based on testing at deformation rates closer to those experienced during ballistic testing. The technique will permit comparisons between emerging prototype backing materials as well as with historical data on the current clay backing material.
  - Testing was recently completed, and the results will be used to screen potential new backing materials and compare their behavior with the current clay backing material.
- Optimization of Arena Test Data Collection Methodology. JLF is investigating the use of a new methodology, based on

techniques developed by NASA, to improve collection of fragment velocity and spatial distribution data during arena testing.
- The technique utilizes piezoelectric film panels for detection, which immediately reports fragment impact locations to a data recorder and requires no additional work for locating the fragments.
- JLF will use the data collected during this program to assess the feasibility incorporating piezoelectric film sensors as a standard method of collecting fragmentation impact location and velocity data during arena testing. The initial results from this project should be available in early FY17.

Improvements of Live Fire Modeling and Simulation

- Enhanced Modeling of BAD Velocity Field for KE Penetrators. JLF supported the improvement of the behind armor debris (BAD) algorithm by collecting unprecedented, high-speed images of kinetic energy warhead BAD using the pulsed laser illumination system (Figure 4).
  - Three-dimensional analyses of these images produced fragment speeds as a function of the fragment's angle from the residual jet.
  - The test data indicate the scatter of kinetic energy BAD fragments may not be a simple function of cone angle, however the Gaussian velocity field used in the BAD algorithm is an improvement over the previous function. Based on the results of this project, the Gaussian velocity filed will be used to represent kinetic energy BAD fragment velocities.

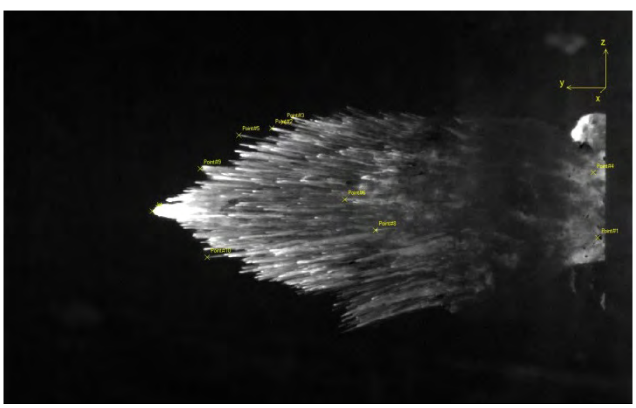


Figure 4. High-speed image of BAD fragments

- Joint Light Tactical Vehicle (JLTV) Underbody Blast Vulnerability Assessment. JLF is investigating the use of high-fidelity computational physics models to simulate vehicle underbody blasts at multiple vehicle locations with several threat sizes. This approach will improve the ground survivability community's understanding of vehicle structural response and occupant injury risk for various threat size and blast location scenarios.
  - JLF will perform system-level underbody blast simulations on the JLTV in at least 12 blast locations using up to 3 sizes of threat and assess the results against the DOT&E survivability criteria used for the JLTV program (see Figure 5). The high fidelity mesh model to support these simulations is in development.
  - This modeling approach would represent a new assessment capability: a multi-threat and multi-location methodology for mapping vehicle structural response and occupant injury risk of combat systems. Performing simulations at multiple threat locations should show the changes in vulnerability across different regions of the underbody, while simulating different charge sizes will help identify the estimates of most vulnerable underbody areas to increasing threat size.

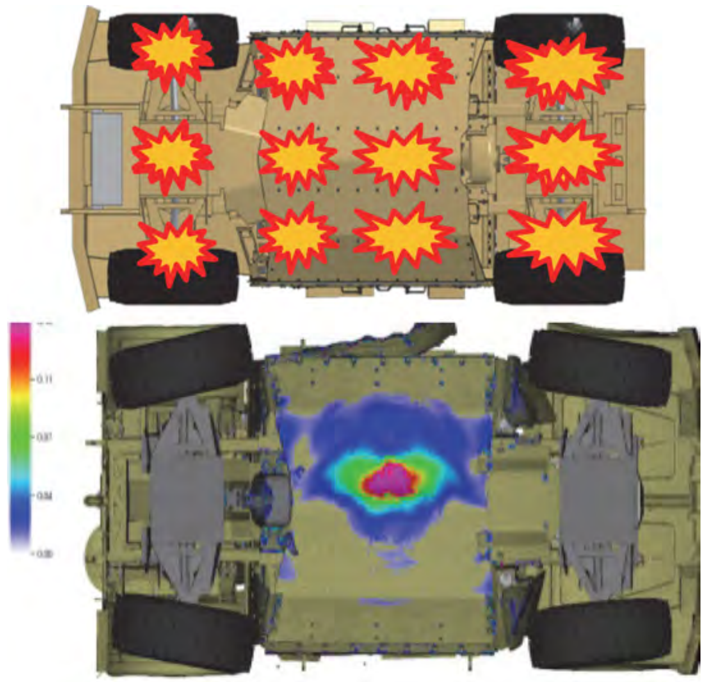


Figure 5. Shotline selection for simulations (top) and structural response of vehicle underbody (bottom)

- JLF supported the development of a shaped charge jets effects model.
  - Initiation of stowed 25 mm ammunition is one of several lethal mechanisms that can impart catastrophic levels of damage to a ground vehicle. Testing on stowed 25 mm training rounds with shaped-charge jets of varying size and velocity collected quasi-static pressure versus time data that will be used to develop a new ammunition compartment vulnerability model.
- JLF continued a joint effort with Germany to develop and validate the Dynamic Systems Mechanical Advanced Simulation (DYSMAS) hydrocode used to model bottom and near-bottom underwater explosions effects.
  - In FY14, several tests were conducted in the Briar Point test pond at the Aberdeen Test Center, Maryland, using a floating shock platform to collect data on platform response from charges located at mid-depth, near-bottom, and on the bottom.
  - The analysis of those test results was completed in FY15, providing additional validation for the use of DYSMAS in vulnerability assessments for the modeling of underwater

explosion loading and ship responses in littoral or harbor environments, where bottomed or tethered mines are likely to be encountered. DYSMAS predictions are improved with the use of sea-bottom data for the location of interest.

- JLF continued to investigate sea-based weapons effects phenomena to improve the fidelity of modeling and simulation used to assess both platform survivability and weapon effects.
  - In FY16, work continued to improve the understanding of combined shock and submergence effects from underwater explosions on unique submarine structural configurations when at deep depths. Scaled test models were fabricated in preparation for FY17 testing. The data from these tests will be correlated with modeling and simulation results to determine which models are best for assessing underwater explosion shock loads in combination with submergence pressure loadings on submarines.
  - In FY16, JLF developed a plan to conduct a collaborative research and test effort with the Canadian Navy to improve the ability to model the effects of near-field underwater explosions and the resulting bubble and bubble jetting loading on structural damage. The data gathered will validate modeling and simulation tools used to evaluate the survivability of Navy platforms against torpedo and mine threats and to improve weapon lethality estimates.

LFT&E SPECIAL INTEREST PROGRAMS

Warrior Injury Assessment Manikin

- The Warrior Injury Assessment Manikin (WIAMan) Engineering Office (WEO) is currently leading the WIAMan project (Figure 6) on behalf of the Army Research, Development, and Engineering Command (RDECOM), with the Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) supporting acquisition-related preparation activities. RDECOM and PEO STRI signed a memorandum of agreement defining the leadership, responsibilities, and funding relationships between these two organizations.
  - The WIAMan project will enter the acquisition cycle as a post-Milestone A program of record via a Materiel Development Decision in FY17. The WEO will transition leadership of the WIAMan project to PEO STRI at Milestone B, but will continue to support PEO STRI in certain non-severable activities related to the WEO's expertise in biomechanics, anthropomorphic test device (ATD) development, and Live Fire Test and Evaluation (LFT&E).
  - The Army developed and validated a Test Capability Requirements Document (TCRD) for the WIAMan project. The Army Test and Evaluation Command, RDECOM, and DOT&E all signed the TCRD. The TCRD identifies the key performance parameters, key system attributes, and requirements for the WIAMan ATD system. In addition to the development of a validated TCRD, the WIAMan project held an Industry Day in June 2016 in order to gauge the level of interest and available competition in the ATD industrial base.
  - The WEO continued to demonstrate that the current ATD used in LFT&E, the Hybrid III, lacks biofidelity in the underbody blast (UBB) test environment, meaning it does not exhibit a human-like response when exposed to UBB loading conditions. ATD biofidelity is assessed via compliance with biofidelity response corridors (BRCs) for the human body regions and response parameters of interest.
  - In FY16, the project delivered the remaining 13 component-level BRCs. These BRCs are focused on the human response in the head/neck, lumbar spine, pelvis, and lower leg/foot and ankle body regions.
  - The project delivered 6 of 12 whole-body BRCs. These BRCs focused on human response to different combinations of parameters that vary in LFT&E, such as loading rate inputs, occupant posture, and Personal Protective Equipment. The remaining whole-body BRCs will be developed in FY17.
  - The project generated initial data on the tolerance of bones to severe loading conditions and developed a notional human injury probability curve (HIPC) for foot and ankle fractures. The WEO also conducted a prioritization exercise that benefitted from updated analyses of injuries experienced by soldiers in combat; this exercise resulted in an executable biomechanics test plan that will result in no less than 36 unique HIPCs, spanning the head, neck, lumbar spine, pelvis, leg, and foot/ankle body regions.
- In FY16, the WEO initiated a 3-year, $3 Million pilot study to investigate the effects of the UBB environment on female soldiers. The objective of this study is to determine if UBB loading conditions affect females differently than males and, if so, for what reasons. The results of this pilot study will be used to inform a decision about the need to develop unique injury assessment capability for female Soldiers. A total of 5 whole body female biomechanics tests were executed in FY16, with an additional 13-17 planned for FY17.
- The WEO continued to implement emerging biomechanics data into the development of a WIAMan ATD through new task order awards to Diversified Technical Systems (DTS). In FY16 DTS delivered a Technology Demonstrator ATD that demonstrated improved biofidelity and usability in the UBB test environment when compared to the Hybrid III ATD. Test results to date indicate that the WIAMan Project is on track to achieve a Technology Readiness Level 6 prior to program transition at Milestone B. DTS also delivered the first data acquisition system (DAS) units for benchtop testing in September 2016, and will deliver four fully integrated first generation WIAMan ATD prototypes for verification and validation testing in June 2017.

- The WEO continued its refinement of an optimized ATD finite element model. This model supported analyses to accelerate the redesign of the ATD to achieve strength-of-design, biofidelity, and usability goals. A full three-dimensional description of the ATD has been created and validated in accordance with the current Technology Demonstrator design and performance.
- The WEO continues to accomplish its technical goals regarding establishing human body response to the UBB load regime, to include expanding its investigation into potential gender-based differences. The Assistant Secretary of Defense for Health Affairs has committed to fully funding the medical research required to meet the WEO's scientific goals. However, the planning and execution of the formal acquisition program envisioned by the Army is behind schedule, while incurring significant overhead costs. Despite the Army's and the Department's large investment in this project, the Army's concerns about the cost of procuring and incorporating this much-needed technological advancement into UBB LFT&E have resulted in no acquisition funding programmed for the project after FY18.

Figure 6. WIAMan Technology Demonstrator

Homemade Explosives

DOT&E continued to participate in the Army-led, multi-Service effort known as the Homemade Explosives Characterization (HME-C) working group. The HME-C effort originated to address concerns regarding the Department's ability to test operationally significant scenarios involving underbody blast threats, and to ensure adequate LFT&E of military vehicles now and in the future. In FY16:

- The HME-C working group completed the planned scope of test and evaluated the data resulting from all of the program's test phases.
- DOT&E used the information and data to develop LFT&E policy for employing buried underbody blast surrogates. This included a new soil standard for use with underbody blast testing.
- The Army Test and Evaluation Command developed operating procedures to implement this policy.

Small Boat Shooters' Working Group

Small boats represent a growing threat class to ships operating in littoral waters and are targeted by a wide variety of weapons systems.

- In FY16, DOT&E sponsored the fifth annual Small Boat Shooters' Working Group, which examined the general nature of the small boat threat in littoral waters; summarized the threat classes and available targets and models available for ammunition, rocket, and tactical missile weapon systems; and attempted to synchronize various LFT&E and other operational test approaches among the various programs/Services by sharing the breadth of test and evaluation options available to evaluators.
- The working group assessed the nature of the small boat threat; the availability of targets and lethality models representing those threats; the data collection, test techniques, and instrumentation that have been applied to small boats; and the performance of shipboard and aircraft weapons against small boat threats. The group also reviewed results from DDG-1000 gun tests, a test concept for HELLFIRE longbow missiles vertically fired from a ship against High-Speed Mobile Surface Targets (as part of the Littoral Combat Ship (LCS) program), and results from tests of special 30 mm gun ammunition under development specifically to counter the small boat threat.

Helicopter Seating Systems

The House Report accompanying the National Defense Authorization Act for FY16 required a briefing describing any plans for improvements to current helicopter seating systems. DOT&E briefed Congressional staff that, while improved helicopter seating would improve force protection, it is just one aspect of the overall helicopter force protection/survivability improvement effort. Addressing leading causes of fatalities in mishaps and combat-induced crashes with near-term technology solutions such as controlled flight into terrain collision and threat avoidance would provide a higher payoff.

- The leading causes of mishaps and combat-induced casualties cannot be mitigated via improved helicopter seating systems.
  - The leading cause of mishaps is controlled flight into terrain due to loss of situational awareness. These events are typically not survivable but could be mitigated through implementation of crash avoidance technologies. Crash avoidance technology has been demonstrated on the UH-1N at technology readiness level 9 (use in operational conditions). If crash avoidance requirements are set, solutions could be fielded on existing systems.
  - The leading causes of helicopter combat-induced casualties are aircraft vulnerabilities leading to catastrophic crashes that are not survivable. These crashes could be mitigated through improved situational awareness, adaptive flight

control, and countermeasure technologies. Additional RDT&E investments in these areas are warranted.

- In many survivable crashes, helicopter seating systems provide adequate protection for the pilot/crew but not for troops and passengers. The troop seating system standard has been waived to enable mission performance. Therefore, existing troop seating systems do not meet the military standards, resulting in preventable casualties.
- Current helicopter seating system ergonomics may be detrimental to mission effectiveness and result in long term disability, but the extent and exact causes have not been determined. Additional analysis is warranted to determine the root cause of casualties, especially to troops and passengers, and the root cause of long-term disabilities.
- DOT&E recommended identifying and addressing the root causes of crew casualties in mishaps and combat-induced crashes and funding the systems that have the greatest return on investment for avoiding or reducing fatalities and injuries.

Cybersecurity

Cybersecurity

Cybersecurity

SUMMARY

DOT&E provides cybersecurity evaluations of DOD acquisition programs as part of the programs' operational test and evaluation. In addition, Congress directed DOT&E to perform cybersecurity assessments of live, operational DOD networks and systems during Combatant Command (CCMD) and Service training exercises. This report includes results from FY16 assessments, but pays particular attention to the trends and changes that have occurred since 2009, when DOT&E updated and improved the requirements and procedures for cybersecurity test and evaluation. Key observations follow, and additional details are in the classified cybersecurity report DOT&E issued in July 2016:

- Over the last 7 years, the Department has increased its focus on cybersecurity, and allocated additional resources to cyber capabilities, expertise, and associated activities. As a result, in recent years some DOD programs and networks have demonstrated, for the first time, effective defenses against attacks from cyber Red Teams emulating threats with limited cyber capabilities. In recent years, DOT&E's cybersecurity assessment program has helped CCMDs address major cybersecurity vulnerabilities through its focus on finding vulnerabilities, helping the CCMD to fix the vulnerabilities, and independently verifying that the vulnerabilities have indeed been fixed. This "find-fix-verify" approach has proven to be an effective way to rapidly improve the cybersecurity of DOD programs and networks.
- Despite this progress, during major exercises critical CCMD missions remain at risk when subjected to cyber-attacks emulating an advanced nation-state adversary. Cyber-attacks are clearly a part of modern warfare, and DOD networks are constantly under attack. However, DOD personnel too often treat network defense as an administrative function, not a warfighting capability. Until this paradigm changes, and the change is reflected in the Department's approach to cybersecurity personnel, resource allocation, training, accountability, and program and network management, the Department will continue to struggle to adequately defend its systems and networks from advanced cyber-attacks.
- DOT&E issued more explicit policy and guidance regarding cybersecurity testing over the past 7 years, resulting in a significant increase in the cybersecurity component of OT&E for major programs. Most operational tests have found significant vulnerabilities and limitations in the system's ability to sustain missions or rapidly restore capabilities when compromised.
- Over the past 7 years, Red Team operators have become high-demand, low-density assets, and requests for Red Team services increasingly go unsatisfied. DOD had an enviable share of master-level operators 7 years ago, but a significant number of these cyber experts accepted positions in the private sector in the ensuing years, often because of the increased wages and more relaxed work environment. Simultaneously, demand within DOD for Red Team services has more than doubled. The new congressional requirement to conduct cybersecurity assessments of all major DOD programs (Section 1647 of the FY16 NDAA) will increase further the demand on DOD Red Teams. Additionally, Red Team capabilities and expertise must increase so that the teams can emulate more advanced and realistic adversaries during testing and training.
- Over the last 3 years, DOT&E refined and expanded the use of long-duration cyber Red Teaming in CCMD networks, including U.S. Pacific Command (USPACOM) and U.S. Northern Command (USNORTHCOM). Such long-duration Red Teaming, conducted by a Persistent Cyber Opposing Force (PCO), is far better at emulating advanced, persistent nation-state cyber threats, while at the same time more efficiently utilizing scarce Red Team resources. PCO activities have identified, and rapidly addressed, serious vulnerabilities that had not previously been discovered during more than a decade of short-duration, less realistic exercise events.
- To effectively fight a war in cyberspace, the focus of cyber defense needs to expand beyond the traditional approaches of system protection and intrusion detection to encompass a broader view of system resilience. DOD has focused a great deal of attention and resources on the defense of outward-facing boundaries. As a result, these boundaries have shown significant improvement in protecting against nascent- and limited-level attacks. However, Red Teams emulating a moderate-level adversary – or below – routinely demonstrate the ability to intrude DOD networks and operate undetected within DOD networks for extended periods of time. The Department needs to put more emphasis on preventing lateral movement by network intruders and improved detection of anomalous network activity.
- In recent years, CCMDs and Services have provided better opportunities for DOT&E-sponsored assessments to inject limited cyber-attacks and observe the resulting effects and responses. However, exercise and network authorities seldom allow fully representative cyber-attacks, and complete assessments of protection, detection, and response capabilities.
- Cyber ranges can be effective venues to fully evaluate realistic cyber-attacks and defenses in a safe and secure environment, without any risk to DOD operations and missions. Cyber ranges may be the only acceptable environment where Red Teams can fully execute attacks representative of an advanced nation-state cyber adversary. Over the last 7 years, DOD has matured its cyber range capabilities, but existing ranges will not be able to fully support the anticipated near-term requirements, including: needed training for the Cyber Mission Forces (CMF), more realistic CCMD and Service exercises and assessments, and rapidly increasing acquisition

program cyber testing requirements. Recent investments in the Persistent Training Environment and Cyber Test Ranges should help remedy these shortfalls, but improvements are likely to remain sub-optimized due to lack of a single Executive Agent for cyber ranges.

- While some Cyber Protection Team (CPT) elements have successfully defended DOD networks during our assessments, many of the 68 CPTs have not received adequate training or equipment to provide effective and timely support to defend networks and critical missions. The initial staffing of the CPT included personnel without the requisite skills and training, and with many current CPT members scheduled to depart in the next year, DOD needs to focus on attracting, training, and retaining skilled individuals for the CPT. DOT&E has provided excellent training opportunities for CPT members during our assessments, and we plan to work with U.S. Cyber Command (USCYBERCOM) to identify more opportunities to do so in the future.
- Over the last 7 years, CCMDs have become increasingly interested in Offensive Cyber Operations (OCO) capabilities. However, CCMDs often have little confidence in available OCO capabilities because the OCO developers have not tested the capabilities in a realistic environment. DOT&E sponsored several test events in FY16 to demonstrate that more realistic testing of OCO capabilities can be both expeditious and low-cost. These events demonstrated that realistic testing of OCO can reveal significant operational problems which do not surface during limited lab testing. The OCO developers can then address these problems to make the capability more likely to succeed when it is deployed. Realistic OCO testing also enabled DOT&E to provide CCMDs with an improved understanding of the scope and duration of OCO effects.
- In recent operational tests, DOT&E has frequently encountered two components that are prevalent across many DOD acquisition programs: Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDSs). These components can introduce cyber vulnerabilities to the system under test and the associated network(s). DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing to help identify vulnerabilities, potential mitigation strategies, and rigorous methods for testing these components.

Table 1 below shows the operational tests involving cybersecurity, and the DOT&E-funded cybersecurity assessments conducted during FY16. Table 2 shows the cybersecurity test organizations that supported the conduct of the activities shown in Table 1.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY16		
EVENT TYPE	SYSTEM OR ORGANIZATION	
Cybersecurity Operational Test	Automated Biometric Information System	F-35 Joint Strike Fighter – Central Point of Entry
	AC130-J Ghostrider	F-35 Joint Strike Fighter – Squadron Kit
	Aegis Ashore	Joint Stand-Off Weapon
	Advanced Field Artillery Tactical Data System	Joint Warning and Reporting Network
	Army Integrated Air and Missile Defense	Littoral Combat Ship
	Acoustic Rapid Commercial-off-the-Shelf Insertion	LHA 6 - America Class - Amphibious Assault Ship
	Airborne Warning and Control System	MQ-9 Reaper
	Aegis Weapons System	Mobile User Objective System
	Common Aviation Command and Control System	Next Generation Diagnostic System
	Consolidated Afloat Network and Enterprise Services	Network Integration Event
	CV-22 Osprey	Navy Advanced Extremely High Frequency Multi-band Term.
	Defense Agency Initiative	Near Real Time Identity Operations
	Distributed Common Ground System – Navy	Pueblo Chemical Agent Destruction Pilot Plant
	Defense Medical Information Exchange	Paladin Integrated Management
	E-2D Advanced Hawkeye	Public Key Infrastructure
	Expeditionary Sea Base	RQ-4 Global Hawk
	Global Broadcast Service	Space-Based Infrared System
	Global Command and Control System - Joint	Spider XM7 Network Command Munition
	High Mobility Artillery Rocket System	Theater Medical Information Program – Joint
	F-35 Joint Strike Fighter – Air Vehicle	Warfighter Information Network – Tactical
	F-35 Joint Strike Fighter – Autonomic Logistics Operating Unit	
Exercise Assessments	U.S. Africa Command Epic Guardian 2016	U.S. Special Operations Command Jackal Stone 2016
	U.S. Central Command Marine Forces Central	USMC Large Scale Exercise 2016
	U.S. European Command Jackal Stone 2016	U.S. Strategic Command Global Thunder 2016
	U.S. Pacific Command Pacific Sentry 2016	U.S. Strategic Command Global Lightning 2016
	U.S. Southern Command PANAMAX 2016	U.S. Navy Valiant Shield 2016
Cyber Readiness Campaigns	U.S. Northern Command	
	U.S. Pacific Command	

TABLE 2. CYBERSECURITY TEST COMMUNITY	
Operational Test Agencies	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corp Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
Cyber Teams	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
	92nd Cyberspace Operations Squadron
	46th Test Squadron
	18th Flight Test Squadron
	Air Force Information Operations Center
	688 Information Operations Wing
Army	1st Information Operations Command
	Threat Systems Management Office
	Army Research Laboratory Survivability and Lethality Analysis Division
Navy	Navy Information Operations Command
	Space and Naval Warfare Systems Command
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Information Assurance Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Risk Management Executive Red Team

RECOMMENDATIONS

- The Combatant Commands and Services should reduce restrictions that prevent testing and training against realistic cyber threats, and perform "fight-through" events to demonstrate that their critical missions are resilient in contested cyber environments.
- The Joint Staff should sponsor a cyber-focused exercise with a different CCMD each year, where cyber training and mission resiliency are the primary training objectives.
- The Services should upgrade their cyber Red Teams with additional capacity, capabilities, training, and threat assessments to ensure that the certified Red Teams can portray relevant and representative adversaries, including advanced nation-state threats.
- The DOD Chief Information Officer and USCYBERCOM should issue policy and instructions to require implementation of the following as soon as possible; vulnerabilities in these areas often jeopardize CCMD and acquisition program missions during cybersecurity assessments and operational tests:
  - Secure credential use and storage
  - Segregation of network privileges, to include role-based allocation of privileged accounts and responsibilities, and network segmentation based on the segments' mission criticality
  - Reduction of cross-connections between networks, and effective, active defense of cross-connections which cannot be eliminated
  - Encryption of data at rest and in transit
  - Centralized logging and audit log correlation to enable rapid detection and tracking of threats inside a system or network
  - Effective anomalous behavior detection, and cyber-attack response tactics and procedures for attacks inside the system or network, as well as at the system/network boundary
  - A consolidated reporting and analysis tool for cyber incidents
  - Locking down SharePoint websites based on "need-to-know"
  - Authentication and verification procedures for chat room participants
- The Joint Staff and USD(AT&L) should require systems and networks to support essential missions even when compromised, and cyber defenders should be able to quickly reset and restore systems and networks following a successful cyber-attack.
- DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel

for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate. The leadership for the Persistent Training Environment and the Cyber Test Range should collaborate to identify priority requirements for range environments in support of testing, training, as well as CCMD and Service exercise assessments.
- DOD should field new cyber capabilities (e.g., Joint Regional Security Stacks, OCO capabilities) only after realistic operational testing confirms the capabilities will be effective and suitable for use by representative users.
- CCMDs and Services should routinely conduct long-duration cyber assessments using a PCO, to enable more threat-representative cyber Red Team activities on DOD networks and to more rapidly discover and address critical cyber vulnerabilities.
- USCYBERCOM, the Services, and Defense Information Systems Agency should conduct "hands-on" training in realistic networks using realistic cyber threats, and effective tools and procedures, for Cyber Mission Force (CMF) personnel and Cybersecurity Service Providers.
- USD(AT&L) and DOD CIO should sponsor the development of test tools and procedures for evaluating cybersecurity in non-Internet Protocol applications, including CDSs, PLCs, system-unique data buses and protocols, radio and acoustic frequencies, and tactical datalinks.

EVOLVING GUIDANCE AND TEST/ASSESSMENT TRENDS

In FY03, the Congress directed DOT&E to perform annual operational evaluations of information assurance with each of the CCMDs and Services; develop a process to similarly consider systems on the DOT&E oversight list; and report to Congress on the Information Assurance (IA) posture of the DOD. DOT&E has performed the required assessments annually since that time, and has in recent years issued and enforced new policy for cybersecurity OT&E.

Early assessments were generally network-focused, with extensive limitations on the supporting Red Teams. Today DOT&E observes fewer limits and restrictions on cybersecurity testing and assessments, but actual impacts to networks and systems are still limited due to safety, security, or other training requirements. The result is that warfighters generally train and conduct cyber assessments in a relatively benign cyber environment.

DOT&E issued the first guidance on cybersecurity requirements for OT&E in 2009, establishing requirements and procedures for testing cybersecurity. Over the past 7 years, that focus has expanded from information-handling systems to encompass a variety of weapons and weapons platforms, and the missions they support.

In 2011, ADM Mullen, the CJCS, issued an Execute Order (EXORD) that directed all CCMDs perform threat-representative assessments of critical CCMD missions in cyber-contested environments within a 3-year period. This EXORD charged exercise authorities and CCMD leadership to conduct major training exercises in a non-benign cyber environment. Exercise authorities now expected cyber Red Teams to participate during exercises, but CCMDs did not consider cyber to be a training objective, and hence cyber activities were severely limited. The Secretary of Defense Leon Panetta re-emphasized the CJCS EXORD in 2012, but this emphasis was soon diluted due to the downsizing and cancelation of exercises due to sequestration.

In 2013, DOT&E and USPACOM agreed that the Department needed to break from the notion that cyber training and assessment performed once a year was acceptable. As a result, DOT&E developed a new approach that includes multiple building-block events in a given year – a Cyber Readiness Campaign – that leads to a culminating event (e.g., a full CCMD exercise), and employs a PCO to emulate a realistic nation-state cyber adversary.

In 2013, USCYBERCOM created the Cyber Mission Force (CMF), consisting of 133 teams. USCYBERCOM and the Services did not have mature plans for training and equipping the CMF. This became evident during DOT&E-sponsored cyber assessments when CCMDs requested Cyber Protection Team (CPT) support, and CPTs were often slow to deploy and unable to provide much support when they arrived. This is still the case for many of the CPTs; however, more recently, DOT&E observed several instances where the CPTs working with hunt teams performed well in detecting and responding to Red Team intrusions. DOT&E will continue to encourage participation of CPT personnel in DOT&E-sponsored Cyber Readiness Campaigns and cybersecurity assessments, where CPTs receive much-needed "hands-on" network training while defending against a realistic cyber adversary.

Concerned with the lack of cybersecurity guidance for acquisition programs, in 2014 DOT&E recommended that the Department develop a cybersecurity requirement. In response, in November 2014 the Deputy Secretary directed the Joint Staff to develop such a requirement within 90 days. Over the past 2 years, the Joint Staff drafted a Cybersecurity Endorsement to the Survivability Key Performance Parameter. The Joint Staff also developed an implementation guide, which identifies a number of key attributes pertaining to cybersecurity that the Services must address in the requirements documentation for systems that handle digital data transfers. These attributes include the ability of the system to control access, reduce detectability, harden attack surfaces, encrypt data, detect anomalies, and recover from a cybersecurity incident. Although the cybersecurity endorsement has been in a draft form for months, the JROC has not yet formally approved and issued it.

In 2015, Secretary Carter issued the DOD Cyber Strategy. This coincided with a number of well-publicized cyber-attacks of government and private organizations, including the breach of the Office of Personnel Management records involving millions of federal personnel. These cyber-attacks helped DOD senior leadership understand the importance of cybersecurity and created opportunities for DOT&E to portray more realistic cyber adversaries during operational tests and exercises.

Despite progress, operational test and exercise planners need to encourage the use of realistic cyber actions that could require restoration of systems or implementation of alternative means of operations. The reluctance to permit debilitating cyber-attacks is appropriate when there are personnel safety concerns, but the DOD needs to routinely assess the ability of missions and systems to either operate through cyber-attacks or restore operations afterwards. Training in a benign environment is not acceptable in any other warfighting domain, nor should it be for cyber.

The DOD should continue to lessen restrictions that prevent testing and training against realistic cyber threats in order to improve the resistance and resilience of mission and systems under conditions that increasingly are part of the daily operational environment.

PROGRESS AND CHALLENGES

Cyber Defenses Continue to Lag Cyber Threats

Over the last 7 years, DOT&E observed and reported on the gradual improvement of defensive capabilities within the Department. The levels of compliance with key cybersecurity practices and controls improved steadily for several years, and test events show that the majority of DOT&E-assessed systems and networks meet key cybersecurity compliance criteria. Nonetheless, DOD cyber Red Teams continue to compromise DOD systems and networks and jeopardize critical DOD missions during exercises. This is because mere compliance with cybersecurity controls is not enough to provide an effective cyber defense. An effective cyber defense requires well-trained, well-equipped cyber defenders, operating in a secure network environment, in conjunction with other warfighters, to maintain critical missions.

Focus Shift to Cyber Resilience: "Assume Breach"

Most cyber defense tools and systems focus on hardening network and system boundaries. When network configurations are up to standard and patches are current, DOD networks can usually withstand cyber-attacks from Red Teams using limited cyber-attack capabilities. Over the past 7 years, the DOD has hardened many of its networks and systems against cyber-attacks by more rapidly installing security patches and improving the security of credentials (such as passwords). This has helped prevent Red Teams using novice techniques from penetrating network and system boundary defenses and disrupting missions during exercises. However, Red Teams using more advanced techniques continue to demonstrate the ability to bypass boundary protections, intrude into DOD networks, and operate undetected for extended periods.

Once they have gained access to a network, Red Teams frequently use tools native to the network and stolen credentials. These two tactics seriously challenge defenders, as they do not currently have sensors or tools to determine that an adversary is using tools or credentials approved for that network; in order to identify an adversary presence, they must detect some anomalous activity or behavior. Anomalous behavior detection is a critical element of cybersecurity, but few DOD cyber defenders have the tools needed to accomplish this.

Coordination and communication among the many agencies and activities charged with providing cyber defenses is often inefficient or ineffective. This lack of coordination contributed to missed opportunities to detect Red Team activities.

DOD should prepare for potential adversaries who may employ advanced capabilities and techniques by developing "fight-through" capabilities. CCMDs and Services should perform frequent training in cyber-contested environments that emphasizes well-coordinated cyber responses, the ability to reset or restore networks and systems to operation following an attack, and the ability of the warfighter to complete assigned missions while under cyber-attack.

Maturing the Cyber Ranges

The DOD Enterprise Cyber Range Environment is a collection of four independent cyber-range assets where classified training and testing can occur. In 2011, these ranges were experiencing budget cuts and were becoming unsustainable. DOT&E proposed enhancements for these cyber ranges and the establishment of an Executive Agent in 2012; as a result, the cyber ranges received additional funding during the FY13 Program Review, but there was no decision for an Executive Agent.

The FY15 NDAA directed DOD to establish an Executive Agent for cyber training ranges and an Executive Agent for cyber testing ranges. In FY16, the DOD allocated funds separately for a Persistent Training Environment, and for cyber test ranges. As combined testing and training are necessary for efficient use of the ranges, and to help address the rapidly increasing demand for cyber range resources, the creation of two separate Executive Agents—with separate responsibilities and funding—may hinder the Department's ability to effectively respond to rapidly evolving and increasingly sophisticated cyber threats. The DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate.

Over the past 2 years, the Test Resources Management Center (TRMC) delivered multiple Regional Service Delivery Points (RSDPs) to key geographical locations, including USPACOM and MIT Lincoln Labs. RSDPs bring cyber range capabilities to local users to permit cost effective testing and training, and they provide a variety of capabilities (instrumentation, traffic generation, environments, etc.) on the local "mini cloud" to reduce the bandwidth requirements for distributed range events. The TRMC also upgraded the National Cyber Range (NCR), and plans to build additional NCR facilities to help meet the rapidly growing demand for cyber test and training resources.

Assisted by DOT&E funding, over the last few years several of the National Labs demonstrated advances in the creation of realistic range environments, including environments that can be quickly built and deployed to an RSDP, the NCR, or other suitable range locations to support testing, training, and CCMD assessments that are not suitable for operational networks. DOD needs more of these environments to adequately test and train against advanced cyber threats.

Joint Information Environment Testing Shortfalls

In 2013, the Chairman of the Joint Chiefs of Staff signed a white paper entitled "Joint Information Environment" identifying "IT efficiencies" as a key goal. This white paper proposed a "shared Information Technology (IT) infrastructure with a common set of enterprise services, under a single security architecture." Subsequently, the DOD CIO established the Joint Information Environment (JIE) as a "concept." The DOD CIO intends all DOD networks to eventually conform to the JIE concept. Hence, the cybersecurity of the JIE concept is critical to the future security of the entire Department. Unfortunately, there is little evidence that JIE will improve cybersecurity, especially if Services field JIE components without adequate preparation in order to meet IT efficiency targets.

JIE is not a formal program of record, and it lacks a unified program executive to manage cost and schedule, monitor performance metrics, and plan and conduct testing. Furthermore, DISA and the Services are pursuing a non-traditional acquisition approach for major JIE components such as the Joint Regional Security Stack (JRSS), and both the Army and Air Force have fielded JRSS without conducting operational testing, despite developmental tests that showed cyber defenders could not use JRSS effectively to defend their network. See the JIE section elsewhere in this annual report for more details.

Although cyber defenders need improved tools to meet the evolving cyber threats, the DOD should not field tools such as JRSS until testing confirms that the tools are effective and usable by representative defenders.

Testing Offensive Cyber Capabilities

Combatant Commands are increasingly interested in Offensive Cyber Operations (OCO) capabilities either as a complement or as an alternative to traditional military capabilities. Factors that prevent CCMDs from adopting OCO capabilities into plans and operations include:

- Timelines for OCO approval that are unacceptably long;
- Waived testing or tests with limited operational realism, and;
- Lack of confirmed and well-characterized knowledge of OCO effects and potential risks.

OCO developers may waive tests because they consider testing as an unacceptable cost in terms of time and money. Waiving such tests occurs despite the fact that extended approval timelines for OCO result in part from the failure to conduct testing to rigorously characterize OCO effects and risks. What policy and guidance does exist for OCO capabilities emphasizes technical specifications, rather than the operational performance and suitability of the tool in a realistic environment. Many OCO capabilities undergo only limited testing, and seldom do any of these tests approach the rigor or realism of an operational test.

DOT&E sponsored several test events in FY16 for selected OCO capabilities at the request of Combatant Commands who had interest in advertised capabilities, but were unsure how much confidence to place in the scope and duration of the desired effects. These events demonstrated that testing of OCO capabilities can be both expeditious and low-cost. The test findings based on end-to-end employment with a cognitive cyber adversary differed greatly from the limited lab testing results. DOT&E-sponsored test results motivated improvements to OCO capability performance and reductions in undesirable second- and third-order effects.

OCO development and release authorities should conduct rigorous operational testing on OCO capabilities when the capabilities are complex and likely to be employed, and/or the risks of failure are unacceptable. DOD should take advantage of the recent advances in high-fidelity cyber ranges to perform more rigorous testing of OCO capabilities. OCO development teams should include test experts in the capability development phase to help validate requirements, focus performance metrics, and expedite a range environment that can support development, testing, and mission rehearsal.

DOT&E will continue to work with US Cyber Command, the Joint Staff, and the Services to enable rigorous OT&E of OCO capabilities. DOT&E will also stand up a cyber element within the Joint Technical Coordinating Group to perform subsequent analysis and reporting of test results to warfighters and DOD leadership.

PATH FORWARD FOR CYBERSECURITY TESTING

Improve Strategic Test Planning

DOT&E has reviewed over 800 documents related to cybersecurity OT&E in the last four years, including Test and Evaluation Master Plans, Operational Test Plans, Emerging Results, and test reports. DOT&E reviewed 240 of these documents in the last calendar year, supporting operational test and evaluation of over 100 systems.

While the quality of cybersecurity test planning continues to improve, program offices and operational test agencies need to place greater emphasis on the following areas in preparing test plans:

- Development and documentation of complete system architectures

- The means for testing non-Internet Protocol technologies
- A description of how cybersecurity tests will demonstrate active defense from attacks, measure the effectiveness of the cyber defenses, and assess the mission impacts resulting from cyber-attacks
- End-to-end testing, to include key subsystems, peripherals, and plug-ins
- Identification of resources (including cyber ranges) to be used for testing
- The role of cybersecurity service providers.

Similarly, test agencies and CCMDs require better master plans to improve the management and objectives of exercise assessments. An acquisition program's TEMP should include and describe the overall plan for cybersecurity test and evaluation. A Cyber Assessment Master Plan (CAMP) is a multi-year plan that identifies the strategic cybersecurity priorities for each CCMD or Service participating in the DOT&E Cybersecurity Assessment Program. CAMPs should focus assessment activities on critical missions that CCMDs must be able to sustain in contested cyber environments, and should motivate fight-through demonstrations in exercises or high-fidelity range events.

As the capabilities of cyber adversaries continue to grow, so must our ability to accurately portray and account for cyber threats in our OT&E and CCMD assessments. To achieve this we will work with the Combatant Commands and Services, and in particular USCYBERCOM, to develop long-term Standing Ground Rules that enable PCO activities. These standing agreements are key to the realistic threat portrayal of advanced adversaries, and offer efficiencies in the application of limited Red Team assets.

Meeting the Need for Cyber Red Teams

The DOD Cyber Strategy and DOT&E policy mandate that operational tests and exercise assessments include representative cyber-threat portrayal. Attainment of this mandate requires sufficient numbers of expert Cyber Red Team operators and supporting cyber planners to assist in the development and execution of operationally realistic cybersecurity tests, the planning and assessment of CCMD exercises and missions, and to support remediation efforts for identified vulnerabilities. The demand on DOD Cyber Red Teams has increased significantly in the past 3 years, and in the same timeframe, the private sector has hired away many members of Cyber Red Teams. As a result, Red Teams are unable to meet current DOD demand. This shortage has caused delays in cybersecurity operational testing, and reduced Red Team capabilities during some CCMD assessments. More critically, the personnel shortage has drastically increased the operational tempo of Red Team members, reducing their training opportunities to the extent that they are not able to keep pace with the tool and skill sets of advanced cyber adversaries. To address this critical situation, the Services should increase the hiring and retention of qualified Red Team personnel, and upgrade their Red Teams with new tools and training to ensure that their teams can portray advanced nation-state adversaries.

DOT&E has created two initiatives to mitigate the impact of Red Team personnel shortages and address the need for more advanced Cyber Red Team support. The PCO organizes existing DOD-certified Red Teams to support long-duration cyber activities that more closely resemble advanced persistent cyber adversaries. USPACOM and USNORTHCOM have signed Standing Ground Rules to implement the PCO construct to provide year-round cyber opposing force support for training and assessment events. The PCO has helped USPACOM find and remediate significant cyber vulnerabilities that might have otherwise gone undetected. Other Combatant Commands are developing agreements to permit PCO activities in their theaters, and DOT&E is coordinating with USCYBERCOM to develop the process and authorities for a global PCO.

DOT&E also created the Advanced Cyber OPFOR (ACO) concept to augment DOD Red Teams with more advanced nation-state capabilities. The ACO enables developers of advanced cyber capabilities and practitioners of advanced techniques to assist in planning and execution of PCO operations.

Testing Fielded Operational Systems

The cybersecurity posture of systems reflects aspects inherent to the system itself, but also aspects that reflect the surrounding operational environment, systems, and cyberspace. Operational testing of acquisition programs enables the evaluation of cybersecurity for systems in development, but fielding of the system following operational testing can result in changes to its cybersecurity posture.

Cybersecurity is a continuing and iterative process, but the DOD has no established mechanism for examining cybersecurity posture of systems following fielding. The DOT&E Cybersecurity Assessment Program examines fielded systems during CCMD and Service exercises, but most are headquarters command and control systems.

Congress recognized this cybersecurity shortfall with the FY16 NDAA Section 1647 language that directed USD AT&L to examine the cybersecurity posture of fielded systems. DOT&E is assisting this effort by providing access to all assessment results and partnerships, and identifying opportunities to conduct Section 1647 assessments in conjunction with CCMD and Service assessments and range events. To develop the Section 1647 assessment plans, the 1647 team used best practices DOT&E developed for cybersecurity operational testing and network assessments.

Resolving Legacy Problems

In conducting tests of already-fielded systems as well as new systems under acquisition oversight, DOT&E has encountered several classes of components (e.g., Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDS)), which could introduce cyber vulnerabilities to the system. Focused cybersecurity testing of such components will identify methods and analytical approaches to apply test results across multiple acquisition programs and achieve potentially significant test efficiencies.

DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing at Sandia National Laboratory, Pacific Northwest National Laboratory, and the MITRE Corporation to help identify rigorous methods for cyber testing these components, vulnerabilities, and potential mitigation strategies for developers and users of systems with these components.

Additionally, DOT&E provided guidance to the Operational Test Agencies regarding areas where cybersecurity OT&E should expand. These include:

- Non-Internet Protocol data buses and formats, to include the Military Standard 1553 bus, the Aeronautical Radio Standard 429, the Controller Area Network bus, and the 700 and 800-series avionics data buses
- Radio frequency, acoustic, radar data, and tactical datalink formats

TABLE 3. PLANNED CYBERSECURITY ASSESSMENT PROGRAM ASSESSMENTS IN FY17

EVENT TYPE	ORGANIZATION	
Exercise Assessments	U.S. Africa Command Judicious Response 2017	U.S. Pacific Command Pacific Sentry 2017
	U.S. European Command Austere Challenge 2017	USMC Large Scale Exercise 2017
Cyber Readiness Campaigns	U.S. Central Command	U.S Air Force Air Operations Centers (to be selected)
	U.S. Northern Command	U.S. Navy Amphibious Ready Group/Marine Expeditionary Group
	U.S. Southern Command	U.S. Army Reserve Command
	U.S. Special Operations Command	U.S. Army Civil Affairs Physiological Operations Command
	U.S. Strategic Command	White Sands Missile Range
	U.S. Transportation Command	

Test and Evaluation Resources

Test and Evaluation Resources

Test and Evaluation Resources

Public law requires DOT&E to assess the adequacy of operational and live fire testing conducted for programs under oversight. This assessment must include comments and recommendations on resources and facilities available for OT&E and LFT&E and on levels of funding made available for these activities. DOT&E monitors and reviews DOD- and Service-level strategic plans, investment programs, and resource management decisions so that capabilities necessary for realistic operational tests are supported. This report highlights areas of concern in testing current and future systems and discusses significant challenges, DOT&E recommendations, and T&E resource and infrastructure needs to support operational and live fire testing. FY16 focus areas include:

- Adjustments to the DOT&E FY16 Budget Request
- Army Support of OT&E
- Cybersecurity Red Team Personnel and Capability Shortfalls
- Threat Representation for OT&E of Space Systems
- High-Altitude Electromagnetic Pulse Test Capability
- Joint Strike Fighter Advanced Electronic Warfare Test Resources
- Point Mugu Sea Test Range Enhancements to Support OT&E of Air Warfare Programs
- Electronic Warfare for Land Combat
- Navy Advanced Electronic Warfare Test Resources and Environments
- Equipping the Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved SeaSparrow Missile Block 2 Operational Testing
- Multi-Stage Supersonic Targets
- Fifth-Generation Aerial Target
- Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems
- Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes
- Missile Warning and Infrared Countermeasure Test Capability Gaps
- Threat Modeling and Simulation to Support Aircraft Survivability Equipment Testing
- Foreign Materiel Acquisition Support for T&E
- Tactical Engagement Simulation with Real Time Casualty Assessment
- Warrior Injury Assessment Manikin
- Testing in Urban Environments
- Biological Defense Testing at West Desert Test Center
- Range Sustainability and Radio Frequency Spectrum

Adjustments to the DOT&E FY16 Budget Request

Action by the House Armed Services Committee (HASC), the Senate Armed Services Committee (SASC), the House Appropriations Committee, and the Senate Appropriations Committee on the FY 2016 budget request included:

- HASC and SASC approval of the President's Budget request in the National Defense Authorization Act for FY16.
- Appropriations increases for:
  - Joint T&E ($10 Million)
  - Threat Resources Analysis ($8 Million)

The Congressional increase for Joint T&E is on track to provide six additional Quick Reaction Tests beyond the six Quick React Tests that were included in the base budget. The increase for Threat Resource Analysis improved threat realism for testing, focusing on the following areas:

- Increased cyber intelligence analyses for characterizing emerging cyberspace threat representations and threat environments
- Analysis for converging electronic warfare (EW) and cyber threats
- Standardized methods for documenting and cataloging cyber threats
- Extended support for development and validation of threat models and simulations to improve their fidelity and availability for T&E

Army Support of OT&E

Beginning with the 2014 Annual Report, DOT&E has expressed concern with the continued budget and staffing reductions at the Army Test & Evaluation Command (ATEC) and the office of the Army Test & Evaluation Executive. During the FY16 DOT&E review of the Army's T&E budget and resources, the Army indicated that there would be further staffing reductions at ATEC's Army Evaluation Center and Operational Test Command through FY19. The Army acknowledged that this may cause increased customer billing rates, the inability to conduct simultaneous operational test events, and longer timelines for the release of test reports. Substantial growth in the areas of autonomy, electronic warfare, cybersecurity, and big data analysis continue to put new demands on the Army T&E workforce and infrastructure. Current funding levels do not support growing T&E analysis capability needs. In addition to staffing reductions, the Army must contend with competition from industry as it struggles to recruit, retain, and grow an analytical and technically competent workforce. DOT&E is concerned that this may impact test planning, execution, and reporting and may result in delayed acquisition decisions. DOT&E will continue to monitor the Army T&E workforce to ensure that it is able to support and not hinder the outcomes of the Army's acquisition programs.

Cybersecurity Red Team Personnel and Capability Shortfalls

DOT&E guidance establishes data and reporting requirements for cybersecurity Red Team involvement in both operational tests of acquisition systems and exercise assessments. The demand on DOD-certified Red Teams, which are the core of the cyber opposing force (OPFOR) teams, has increased significantly in the past 3 years. In the same timeframe, the Cyber Mission Force and private sector have hired away members of Red Teams, resulting in staffing shortfalls at a time when demand is likely to continue to increase. This trend must be reversed if the DOD is to retain the ability to effectively train personnel and assess DOD systems and protective measures against realistic cyber threats. In FY16, the almost non-stop pace of events for all Red Teams challenged their ability to provide complete data sets and complete reports. Without these data and reports, network defenders and trainers will not have the critical inputs they need to develop effective mitigations or perform effective training on new procedures.

DOT&E has already seen instances in which tests were rescheduled or could not be performed as planned due to a lack of available cyber teams authorized to conduct cyber operations on live networks and enclaves. The high operational tempo of the Red Teams has reduced or eliminated opportunities for the teams to train, thereby eroding their ability to ensure their skill level is commensurate with advanced nation state cyber threats. The high operational tempo has also induced a number of experienced Red Team members to seek higher paying, less demanding jobs outside of the Department, further exacerbating the personnel shortfalls.

A number of initiatives would help address the increasing shortfall of qualified cybersecurity Red Team personnel:

- Create pay and other incentives for cybersecurity personnel – such as those afforded to other highly-trained, critical DOD personnel (e.g., pilots) – in order to retain talented Red Team operators
- Expand the number of master-level and journeyman-level Red Team operators, and develop performance-based certification standards to ensure each Red Team is manned with sufficient numbers of qualified operators
- Expand the Persistent Cyber Opposing Force (PCO) to global authorities to provide more long-duration, efficient, flexible, and threat-realistic cyber effects
- Grow Red Team capabilities and infrastructure to better and more efficiently portray advanced cyber threats, and automate the capture of required data
- Develop automated Red Team capabilities that can perform mid-level cyber exploits and identify common cybersecurity vulnerabilities

Threat Representation for OT&E of Space Systems

U.S. adversaries are working to diminish and overcome U.S. military advantage by threatening our space superiority. Although the military Services normally subject space systems to representative natural hazards and space phenomena during the course of integrated testing campaigns, they often inadequately represent a hostile wartime environment during space systems testing. Potential adversaries are relentlessly pursuing offensive space control capabilities. Therefore, the OT&E of space systems must realistically reflect the hostile threats that U.S. space systems will face, and the military Services must provide the additional resources required to conduct such OT&E.

In March 2016, DOT&E provided guidance to military Service acquisition officials and Service operational test agencies (OTAs) to ensure adequate representation of realistic threats in the OT&E of all segments of space systems, including ground control, space-borne, and user equipment. Military Service acquisition officials and OTAs must identify and address the resource and infrastructure limitations that currently constrain our ability to conduct adequate operationally realistic testing of space systems. In addition to the persistent cyber threats which could target all segments of our space systems, our space forces face electronic warfare, kinetic, and directed energy threats. OTAs must insist on current, validated threat assessments for their space systems, and must adequately and realistically represent each of these threats during OT&E.

To ensure operational realism, OTAs must employ actual threat systems when possible in OT&E. If the required threat resources are not available, then the military Service acquisition official and OTA should act in advance of OT&E to develop or procure those resources. If acquisition and employment of actual threats is not practical, would violate U.S. or DOD policy, or would introduce unmitigated and unacceptable operational, security, or safety risks, then OTAs should use realistic, accredited threat surrogates during OT&E in lieu of the actual threat system. If the actual threat system or realistic threat surrogate is not available for OT&E – despite military Service efforts to develop or procure it – then the OTA should employ accredited threat M&S.

To employ actual threat systems and threat surrogates against satellites for OT&E, in cases where risk or policy will limit adequate on-orbit testing, the military Services should fund pre-launch, thermal vacuum chamber (TVAC) testing of either first articles or non-flight, identical "test satellite" articles for cyber, electronic warfare, and directed energy threats. Representative operational crews should operate satellites being threat tested in TVAC for OT&E, using the control segment and capabilities intended for operational employment. If a Service cannot demonstrate realistic threat intensities in a TVAC, the chamber testing should be supplemented by subcomponent testing at realistic threat intensities, with analyses to correlate observed results to system-level effects.

The acquisition and test communities should leverage the space-related expertise and resources of the many U.S. space-related organizations and individuals to mitigate the infrastructure and resource limitations which currently impede DOD's ability to portray realistic space threats in OT&E. For example, test planners should make use of the expertise and resources of organizations such as NASA, the National Reconnaisance Office, the Joint Navigation Warfare Center, the Space Security and Defense Program, the Test Resource Management Center

(TRMC), and adversary tactics organizations such as the 527th Space Aggressor Squadron.

The March 2016 DOT&E guidance recommends the OTAs take immediate steps to improve their ability to adequately represent space threats by: identifying and tracking space threat representation capabilities, including their availability, location, and connectivity; identifying and prioritizing space threat representation gaps, and requesting funding to fill those gaps; documenting space threat operational and system-level concepts of operations (CONOPS) and blue system defensive CONOPS; designating OPFORs for space threat representation in OT&E; and developing M&S capabilities which support the assessment of system- and mission-level impacts of space threats.

TRMC is conducting an assessment to identify the threat environment, current T&E capabilities, and gaps in those T&E capabilities that are needed to support space system T&E requirements. This assessment will provide an estimate of resources required for acquisition programs to sustain operations in a contested space environment. DOT&E requested each Service T&E Executive to brief their plans for threat representation of space systems during the FY16 budget review process. Finally, all space system TEMPs and test plans submitted to DOT&E for approval must include the resources for a thorough representation of potential threats.

High-Altitude Electromagnetic Pulse Test Capability

Military Standard 4023 (MIL-STD-4023), "High-Altitude Electromagnetic Pulse (HEMP) Protection for Military Surface Ships," requires full-ship electromagnetic pulse (EMP) testing to support surface vessel survivability assessments. In addition, since the DDG 51 is expected to be capable of operating in an EMP environment, DDG 51 Ship Specification, Section 407 establishes requirements for DDG 51 EMP Protection. Section 407 states that during the guarantee period of the ship, the Government will conduct a full-ship EMP test to determine the performance of the ship's electronic systems under simulated EMP conditions.

The Navy currently does not have a capability to conduct a survivability assessment of a full ship subjected to EMP effects. Current Navy practice is to conduct limited testing on ship systems and sub-systems, and then extrapolate these results to the entire ship. This testing method does not provide the data needed to adequately assess full ship EMP survivability at sea in an operational mode. Existing EMP modeling and simulation capabilities provide very limited information on ship survivability, with significant uncertainties.

In FY15, the OSD Chemical Biological Radiological and Nuclear Survivability Oversight Group – Nuclear identified a full-ship EMP Threat Level Simulator (TLS) for warships as their most important test capability gap. The Tri-Service Technical Working Group, responsible for the development of MIL STD-4023, agreed that a full-ship EMP TLS is required for warship EMP threat survivability assurance. The Defense Threat Reduction Agency also determined that testing using a full-ship EMP TLS is the best approach to demonstrate ship threat-level EMP protection and mission assurance in accordance with standing Navy requirements. Currently, surface vessel acquisition programs (e.g., DDG 51) have no plans to conduct a full-ship EMP test because the Navy has no capability to do so. In order to address this testing capability shortfall, in FY16 the Naval Sea Systems Command (NAVSEA) has directed the Navy's EMP Program Office to develop a method of using a Low-Level Continuous Wave Illuminator to conduct EMP testing on one to be determined test ship. Evaluation of this trial will help determine the way forward for the development of a full-ship EMP TLS.

In conjunction with NAVSEA, the Defense Threat Reduction Agency has estimated the costs to build a full-ship EMP TLS capability to be $49 – 54 Million. Once operational, the total cost to conduct nine tests is estimated at $17.5 – 18.6 Million. Full-ship EMP TLS testing at sea will support mission assurance by providing test data for EMP modeling and realistic EMP training scenarios for ship crews. At-sea testing using this capability will demonstrate full-ship EMP survivability and support the U.S. nuclear deterrent posture. DOT&E supports all efforts to address current EMP testing shortfalls as soon as possible.

Joint Strike Fighter Advanced Electronic Warfare Test Resources

In February 2012, DOT&E identified significant shortfalls in EW test resources – in particular threat representation on the open-air ranges. This resulted in nearly $500 Million of funding for the Electronic Warfare Infrastructure Improvement Program (EWIIP). EWIIP intended to buy both open- and closed-loop threat emulators for the open-air ranges, provide upgrades to anechoic chambers and the F-35 mission data file reprogramming lab, and provide intelligence products to support the development of the threat emulators.

Significant progress has been made in some instances, while progress is lacking in other areas. The open- and closed-loop threat emulators – in addition to the lab upgrades – are key to the development, testing, and timely fielding of numerous U.S. systems that are critical for operating successfully against near-peer adversary threat systems that exist, are proliferating, or are undergoing an accelerating pace of significant upgrades. The U.S. aircraft and EW systems include the F-35, F-22 Increment 3.2 A/B, B-2 Defensive Management System, Long Range Strike Bomber, and the Next Generation Jammer for the EA-18G. The status of these EW upgrades is displayed in Table 1.

TABLE 1. RECOMMENDATIONS ON ELECTRONIC WARFARE TEST RESOURCES	
DOT&E Recommendation	**Current Status**
Develop a combination of open- and closed-loop emulators in the numbers required for operationally realistic open-air range testing of the Joint Strike Fighter and other systems beginning in 2018.	Both the open- and closed-loop efforts are underway. The open-loop systems are called Radar Signal Emulators (RSEs). EWIIP was scheduled to deliver the first 2 systems in 2016, 12 systems during 2017, and the final 2 in early 2018, for a total of 16 RSEs – in time to support F-35 IOT&E and other testing in 2018 and beyond. Acceptance and integration testing will be conducted during 2016 and 2017; this testing will establish procedures for use of the RSEs in the F-35 IOT&E and provide validation data for the accreditation of the systems for use in OT&E. Two closed-loop systems are in development but are not scheduled to be available until mid to late 2019, after completion of the planned F 35 IOT&E. The integration architecture developed for the open-loop RSE systems will provide adequate test capabilities for F-35 Block 3F IOT&E, in lieu of closed-loop systems.
Upgrade the Government anechoic chambers with adequate numbers of signal generators for realistic threat density.	Initial studies of materiel solutions to achieve realistic densities have begun. • The Navy chamber has procured improved, interim signal generation capabilities and initial test support equipment for direct signal injection capability for the F-35. Further, the Navy chamber executed F-35 electronic warfare testing for spec compliance and simulation validation in September and October 2016. The facility will introduce a much more substantial upgrade in the summer of 2017 that will allow high-fidelity replication of very high signal density threat environments. • The Air Force chamber has completed one stage of significant hardware upgrades, greatly improving its ability to replicate high signal density environments and has identified a path forward covering more extensive upgrades through 2020.
Upgrade the Joint Strike Fighter mission data file reprogramming lab to include realistic threats in realistic numbers.	A Joint Strike Fighter Program Office-sponsored study to determine upgrade requirements was completed in December 2014. It confirmed the shortfalls identified by DOT&E in February 2012, but also identified many other critical shortfalls preventing effective and efficient mission data file development and reprogramming. Unfortunately, inexplicable delays by the program since this study was completed have ensured that upgrades will not be completed in time to affect mission data file production for Block 3F IOT&E and fielded operations. Also, the program plans to procure fewer signal generators than the study recommended, further jeopardizing the program's ability to generate effective mission data in the future.
Provide Integrated Technical Evaluation and Analysis of Multiple Sources intelligence products needed to guide threat simulations.	Products have been completed and delivered, and are being used to support development of the open- and closed-loop threat radar emulators.

Due to delays and inaction by the F-35 Joint Program Office, the situation at the Joint Strike Fighter mission data file reprogramming lab has resulted in the failure to upgrade the lab before IOT&E of Block 3F capability.

DOT&E believes additional funding of $268 Million is needed for additional range infrastructure for testing, training, and readiness of U.S. aircraft and airborne EW systems. This funding would enable the test ranges and the models and simulations (that must be validated with test data) to assess the performance of U.S. systems against the key challenges of near peer threat air defense networks of the 2020s. These capabilities include: conventional radars with advanced digital signal generation and processing, networked together via advanced track fusion processing systems; multi-static radar networks; passive detection systems; and passive coherent radars. The proposed enhancements are constrained to materiel solutions that can be procured rapidly and off the shelf where possible in order to be available for testing of critical systems such as the Next Generation Jammer.

Point Mugu Sea Test Range Enhancements to Support OT&E of Air Warfare Programs

In 2015 and 2016, DOT&E and USD(AT&L) allocated $22 Million to fund the integration of the Air Warfare Battle Shaping (AWBS) system and the open loop RSEs at Point Mugu Sea Test Range (STR), California. AWBS is a variant of the Air-to-Air Range Instrumentation system at the Air Force Western Test Range (WTR), Nevada, where it is essential for scoring as well as post-mission reconstruction and analysis of OT&E missions. The use of the RSEs at the STR for the F-35 IOT&E provides key operationally realistic scenarios and off-loads some of the F-35 IOT&E trials from the WTR, which can only allocate a few range periods per week for the F-35. Conducting test trials at the STR could considerably shorten the duration of F-35 IOT&E.

In 2016, Navy and Air Force personnel participated together in RSE range integration working groups throughout the year and together with DOT&E observed initial acceptance testing of the first two RSEs. Navy personnel are planning to take part in fall 2016 training for operations, maintenance, and programming of the RSEs. Two RSEs are planned to be temporarily transferred from the Nevada Test and Training Range (NTTR) to the STR during 2017 to complete integration testing at the STR. Eventually, all 16 RSEs will be stationed at NTTR for F-35 IOT&E trials. Once those scenarios are completed, 12 RSEs will move to the STR for additional F-35 IOT&E trials.

Electronic Warfare for Land Combat

Networked mission command systems that support the commander's mission execution across the Brigade Combat Team (BCT) are a cornerstone of the Army's modernization plan. These integrated network capabilities are distributed throughout a combat formation and its support elements, from the brigade command posts down to the individual dismounted soldier. The Army intends commanders, using tactical network systems, to have the ability to transfer information such as voice, video, text, position location information, and high-resolution photographs throughout the BCT, and provide individual commanders access to information needed to complete their mission. The expanded use of radio frequency spectrum to support mission command systems with supporting data networks exposes the BCT to contemporary EW threat vectors available to a broad range of potential enemies. Recent conflicts have demonstrated the mission effects that EW can have on the modern battlefield. As the Army becomes more dependent on these sophisticated network technologies, it is critical that the developmental and operational test communities continue to identify and assess vulnerabilities of these systems. Decision makers must understand the inherent vulnerabilities, as well as the ways in which an enemy may choose to exploit and/or degrade the tactical network.

During operational testing, threat EW is part of a broader combat force that is made available to the opposing force (OPFOR) commander. When possible, the EW systems, tactics, techniques, and procedures employed by the OPFOR during test should represent those of potential adversaries. The Threat Systems Management Office (TSMO) is responsible for developing, operating and sustaining the Army's suite of threat EW capabilities. In early FY17, TSMO will complete the development of three new EW capabilities – to include an upgraded injection jammer, airborne EW payload, and GPS jammer system – demonstrating a continued commitment to providing realistic threat EW for operational test and mitigating limitations when possible. Since they support increased operational realism in testing, these developing threat test capabilities are critical to support future testing of Warfighter Information Network – Tactical Increment 2, Nett Warrior/Rifleman Radio, Mid-Tier Networking Vehicular Radio, Manpack Radio, Joint Battle Command – Platform, and Assured Positioning Navigation and Timing.

Navy Advanced Electronic Warfare Test Resources and Environments

Capability for Realistic Representation of Multiple Anti-Ship Cruise Missile Seekers for Surface Electronic Warfare Improvement Program Operational Testing

This gap in test capability was initially identified in DOT&E's FY13 Annual Report as "Additional Electronic Warfare Simulator Units for Surface Electronic Warfare Improvement Program (SEWIP) Operational Testing." The Navy addressed it with development of a programmable seeker simulator that could represent different Anti-Ship Cruise Missile (ASCM) seekers by specifying the electronic waveform emission characteristics for one of several possible threats. However, the effective radiated power (ERP) was not among those characteristics, resulting in simulated attacks by ASCM representations displaying disparate levels of ERP that are unlikely to be encountered during a stream raid attack of two ASCMs (along the same bearing and elevation and within close proximity of one another). The programmable seeker simulator, termed the "Complex Arbitrary Waveform Synthesizer," needs to be modified such that its ERP more realistically represents the second ASCM of a dual ASCM stream raid.

The next SEWIP Block 2 OT&E is projected for FY19. This is to be followed by FOT&E on a Product Line Architecture-compliant DDG 51 with Block 2 actually integrated with the Aegis Combat System. This integration was not part of the Block 2 IOT&E. Subsequent FOT&E would be with the DDG 1000 and CVN 78 combat systems. The estimated cost to add the ERP improvement is $5 Million. The Navy has not planned for or funded this improvement.

Long-Term Improvement in the Fidelity of Anti-Ship Cruise Missile Seeker/Autopilot Simulators for Electronic Warfare Testing

This gap in test capability was initially identified in DOT&E's FY13 Annual Report due to the continued reliance on manned aircraft for captive-carry of the ASCM seeker simulators. Such simulators will be unable to demonstrate a kinematic response to electronic attack by SEWIP Block 3 nor demonstrate the effect that such kinematic responses will have on ships' hard-kill systems (e.g. missiles, guns). Manned aircraft fly too high and too slowly for credible ASCM representation and are unable to represent ASCM maneuvers. Credible ASCM representation requires a vehicle that can fly at subsonic ASCM speeds and lower altitudes than the current Learjets; can home on a platform representing a SEWIP Block 3-mounted ship, using a threat-representative radar seeker and autopilot; and can respond realistically to Block 3 electronic jamming. An approach to satisfy this requirement is to use a recoverable, unmanned aerial vehicle (UAV) that is equipped with embedded, miniaturized simulators. The UAV should be able to maneuver at ASCM speeds and altitudes with encrypted telemetry to track seeker/autopilot responses to electronic attack. A human-controlled override capability would be required for safe operation. The remotely controlled Self-Defense Test Ship (SDTS) would tow a ship target for the UAVs to home on. SEWIP Block 3 would be mounted on the SDTS along with hard-kill systems such that the integrated hard-kill and soft-kill (i.e., SEWIP Block 3) combat system capability could be demonstrated. Currently, such testing is at the discrete combat system element level, leaving integrated combat system capability unknown.

SEWIP Block 3 IOT&E is projected for FY19. FOT&E of Block 3 integrated with the DDG 1000 combat system, as well as FOT&E with the CVN 78 combat system, should occur subsequent to the IOT&E. The cost for the development of these UAVs (with simulators and telemetry) is estimated to be approximately $120 Million for development, testing, and acquisition. The estimated unit cost of each vehicle is not expected to exceed $15 Million. The Navy has not planned for or funded this improvement.

Equipping the Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved SeaSparrow Missile Block 2 Operational Testing

The close-in ship self-defense battle space is complex and presents a number of challenges. For example, this environment requires:

- Weapon scheduling with very little time for engagement
- The combat system and its sensors to deal with debris fields generated by successful engagements of individual ASCMs within a multi-ASCM raid
- Rapid multi-salvo kill assessments for multiple targets
- Transitions between Evolved SeaSparrow Missile (ESSM) guidance modes
- Conducting ballistic missile defense and area air defense missions (i.e., integrated air and missile defense) while simultaneously conducting ship self-defense
- Contending with stream raids of multiple ASCMs attacking along the same bearing, in which directors illuminate multiple targets (especially true for maneuvering threats)
- Designating targets for destruction by the Close-In Weapons System (CIWS)

Multiple hard-kill weapons systems operate close-in, including the Standard Missile 2, the ESSM, and the CIWS. Soft-kill systems such as the Nulka MK 53 decoy launching system also operate close-in. The short timelines required to conduct successful ship self-defense place great stress on combat system logic, combat system element synchronization, combat system integration, and end-to-end performance.

Navy range safety restrictions prohibit close-in testing on a manned ship because the targets and debris from successful intercepts will pose an unacceptable risk to the ship and personnel at the ranges where these self-defense engagements take place. These restrictions were imposed following a February 1983 incident on the USS *Antrim* (FFG 20), which was struck with a subsonic BQM-74 aerial target during a test of its self-defense weapon systems, killing a civilian instructor. The first unmanned, remotely controlled SDTS – the ex USS *Stoddard* – was put into service that same year. A similar incident occurred in November 2013, in which two sailors were injured when the same type of aerial target struck the USS *Chancellorsville* (CG 62) during what was considered to be a low-risk test of its combat system. This latest incident underscores the inherent dangers of testing with manned ships in the close-in battlespace.

While the investigation into the USS *Chancellorsville* incident has caused the Navy to rethink how it will employ subsonic and supersonic aerial targets near manned ships, the Navy has always considered supersonic ASCM targets a high risk to safety and will not permit flying them directly at a manned ship. The Navy has invested in a current at-sea, unmanned, remotely-controlled test asset (the SDTS) and is using it to overcome these safety restrictions. The Navy is accrediting a high-fidelity modeling and simulation (M&S) capability – utilizing data from the SDTS as well as data from manned ship testing – so that a full assessment of the self-defense capabilities of non-Aegis ships can be completely and affordably conducted. The Navy recognizes that the SDTS is integral to the test programs for certain weapons systems (the Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 1) and ship classes (LPD 17, LHA 6, Littoral Combat Ship, LSD 41/49, DDG 1000, and CVN 78). However, it has not made a similar investment in an SDTS equipped with an Aegis Combat System, Air and Missile Defense Radar (AMDR), and ESSM Block 2 for adequate operational testing of the DDG 51 Flight III Destroyer self-defense capabilities. The current SDTS lacks the appropriate sensors and other combat system elements to test these capabilities.

On September 10, 2014, DOT&E submitted a classified memorandum to USD(AT&L) with a review of the Design of Experiments study by the Navy Program Executive Office for Integrated Warfare Systems. The Navy study attempted to provide a technical justification to show that the test program did not require an SDTS to adequately assess the self-defense capability of the DDG 51 Flight III Class Destroyers. DOT&E found that the study presented a number of flawed justifications and failed to make a cogent argument for why an SDTS is not needed for operational testing.

On December 10, 2014, the Deputy Secretary of Defense (DEPSECDEF) issued a memorandum directing the Director of Cost Assessment and Program Evaluation (CAPE) to identify viable at-sea operational testing options that meet DOT&E adequacy requirements and recommend a course of action (with cost estimates, risks, and benefits) to satisfy testing of the AMDR, Aegis Combat System, and ESSM Block 2 in support of the DDG 51 Flight III Destroyer program. The CAPE study evaluated four options to deliver an at-sea test platform adequate for self-defense operational testing of the DDG 51 Flight III, AMDR, and ESSM Block 2 programs. Each option requires funding beginning in FY18 to ensure support of operational testing of these systems in FY22. A decision on whether to fund the procurement of the needed equipment is pending.

DOT&E continues to recommend equipping an SDTS with capabilities to support Aegis Combat System, AMDR, and ESSM Block 2 OT&E to test ship self-defense systems' performance in the final seconds of the close-in battle and to acquire sufficient data to validate ship self-defense performance M&S. The CAPE-estimated cost for development and acquisition of these capabilities over the Future Years Defense Program is approximately $350 Million. Of that, approximately half could be recouped after the test program completes by installing the hardware in a future DDG 51 Flight III Destroyer hull. The Navy previously agreed with this "re-use" approach in their December 2005 Air Warfare/Ship Self-Defense Test and Evaluation Strategy stating that "… upon completion of testing and when compatible with future test events, refurbish and return the test units to operational condition for re-use."

On February 10, 2016, DEPSECDEF directed the Navy to adjust funds within existing resources to procure long lead items to begin procurement of an SDTS equipped with the Aegis Combat System and AMDR. He further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs. DEPSECDEF required the Navy to document that strategy in a draft TEMP for those programs and submit the TEMP to DOT&E by July 29, 2016. The Navy has complied with the funding direction but has not complied with the DEPSECDEF direction to provide an integrated test strategy for those programs. Despite budgeting for the long lead AMDR components, the Navy has not programmed funding in the Future Years Defense Plan to complete all other activities and equipment required to modify the SDTS to support adequate operational testing of the self-defense capabilities of the DDG 51 Flight III, AMDR, and ESSM Block 2 in FY 2023 as planned.

Multi-Stage Supersonic Targets

The Navy initiated a $297 Million program in 2009 to develop and produce an adequate multi-stage supersonic target (MSST) required for adequate operational testing of Navy surface ship air defense systems. The MSST is critical to the DDG 1000 Destroyer, CVN 78 Aircraft Carrier, DDG 51 Flight III Destroyer, LHA(R), AMDR, Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 2 operational test programs. The MSST underwent restructuring and rebaselining from 2013 – 2015 in order to address technical deficiencies as well as cost and schedule breaches, which would have postponed its initial operational capability to 2020 and increased the total program cost to $962 Million. Based on the restructured/rebaselined MSST program's high cost and schedule delays, as well as new intelligence reports, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) in 2014 directed that alternatives be examined to test against these ASCM threats and subsequently terminated the MSST program. While the details of the final Navy alternative are classified, DOT&E determined that it would be very costly (the Navy estimates $739 Million), very difficult to implement, dependent on the results of highly segmented tests, and would suffer from severe artificialities that would hopelessly confound interpretation of test results. DOT&E informed the Navy that the proposed alternative was not adequate for operational testing and recommended that the Navy not pursue it. MSST aerial target capabilities are still required to complete end-to-end operational testing of Navy surface ship air defense systems and to validate models and simulation capabilities for assessing the probability of raid annihilation for Navy ships.

Fifth-Generation Aerial Target

DOT&E has been investigating the need for an aerial target to adequately represent the characteristics of Fifth Generation threat aircraft in light of the emergence of threat aircraft like Russia's PAK-FA and China's J-20. The Fifth Generation Aerial Target (5GAT) study effort began in 2006 and examined the design and fabrication of a dedicated 5GAT that would be used in the evaluation of U.S. weapon systems effectiveness. The 5GAT team – comprised of Air Force and Navy experts, retired Skunk Works engineers, and industry experts – completed the preliminary design in 2016. The fully owned Government design includes the aircraft outer mold line, internal structures, loads analysis, propulsion, and subsystems. Also, the team built one full-scale, flight-representative wing that will be used for structural load tests and a system integration laboratory. The Department provided funding to complete the final design, tooling, fabrication and flight tests. The prototyping effort will provide cost-informed alternative design and manufacturing approaches for future air vehicle acquisition programs. This data can also be used to assist with future weapon system development decisions as well as T&E planning and investment, and will support future T&E analysis of alternative activities. It will also demonstrate reduced signature, basic aerodynamic performance, and provision for special mission systems.

Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems

Operational testing of anti-submarine warfare (ASW) platforms and related systems includes the ability to detect, evade, counter, and/or destroy an incoming threat torpedo. The determination of system or platform performance is critically dependent on a combination of the characteristics of the incoming torpedo (e.g., dynamics, noise, fusing, sensors, logic, etc.). Due to differences in technological approach and development, U.S. torpedoes are not representative of many highly proliferated torpedoes, particularly those employed in anti-surface warfare by other nations. Contractor, developmental, and operational testing that is limited to U.S. exercise torpedoes will not allow the identification of existing limitations of ASW and related systems against threat torpedoes, and will result in uninformed decisions in the employment of these same systems in wartime. A January 9, 2013, DOT&E memorandum to the ASN(RDA) identifies specific threat torpedo attributes that the threat torpedo surrogate(s) must be evaluated against. A June 18, 2015, DOT&E memorandum to ASN(RDA) reiterated the need for representative threat torpedo surrogates in operational testing and emphasized understanding threat torpedo behavior, including tactics and countermeasure logic, when evaluating the adequacy of torpedo surrogates. A May 24, 2016, DOT&E memorandum to the ASN(RDA) further emphasized the importance of resolving the surrogate shortfall in advance of evaluating the Navy Torpedo Warning System and Countermeasure Anti-torpedo Torpedo acquisitions systems. The non-availability of threat-representative torpedo surrogates will prevent adequate development and operational testing for ASW platforms and related systems, as well as adversely affect tactics development and validation of these tactics within the fleet.

Naval Undersea Warfare Center (NUWC) Division Keyport conducted a study of threat torpedo surrogates in FY14. The $480,000 study was jointly funded by the Navy and DOT&E. The completed study, dated September 4, 2015, confirmed DOT&E concerns that current torpedo surrogates have significant gaps in threat representation for operational testing and provided recommendations for improving current threat torpedo emulation. The Navy has since taken the following actions to address the gaps in threat representation of torpedo surrogates:

- NUWC Division Keyport is currently pursuing a prototype technology development project that will deliver a threat-representative, high speed, quiet propulsion system. The development of a propulsion system prototype is intended to overcome a critical gap identified in the torpedo threat surrogate capability gap analysis, discussed in the preceding paragraph. This effort is funded as an FY16 Resource Enhancement Program project at approximately $1 Million. This project is focused on the propulsion power system but will not address reducing the cavitation noise caused by the surrogate executing operationally realistic threat profiles.
- The Navy proposed development of a General Threat Torpedo (GTT) as a Resource Enhancement Program project for FY17 to provide a torpedo surrogate that better represents threat torpedos in dynamic and acoustic performance, as well as tactical logic. The $6.2 Million project will incorporate the technology developed in the high-speed, quiet propulsion system prototype and is supported by DOT&E. However, the ability of GTT to adequately support operational testing, if developed, will depend on future Navy decisions to procure sufficient quantity of GTT.

Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes

The Navy routinely conducts in-water operational testing of lightweight and heavyweight ASW torpedoes against manned U.S. Navy submarines. Although these exercise torpedoes do not contain explosive warheads, peacetime safety rules require that the weapons run above or below the target submarine with a significant depth stratum offset to avoid collision. While this procedure allows the torpedo to detect, verify, and initiate homing on the target, it does not support assessment of the complete homing and intercept sequence. One additional limitation is the fact that U.S. nuclear attack submarines may not appropriately emulate the active target strength (sonar cross-section) of smaller threats of interest, such as diesel-electric submarines. During the MK 50 lightweight torpedo operational test in May 1992, the Navy conducted some limited set-to-hit testing against manned submarines, which included impact against the target hull, but that practice has been discontinued.

In preparation for the 2004 MK 54 lightweight torpedo operational test, DOT&E supported the development and construction of the unmanned Weapon Set-to-Hit Torpedo Threat Target (WSTTT) using Resource Enhancement Project funding. The WSTTT was a full-sized steel mock-up of a small diesel-electric submarine, with an approximate program cost of $11 Million. As a moored stationary target, the WSTTT could not emulate an evading threat, but its use in the MK 54 operational test demonstrated the value of such a dedicated resource. Unfortunately, the Navy did not properly maintain the WSTTT and abandoned it on the bottom of the sea off the California coast in 2006. In subsequent years, the Navy was able to make some limited use of the WSTTT hulk as a bottomed target for torpedo testing.

In a separate effort, the Navy built the Mobile Anti-Submarine Training Target (MASTT), designed to serve as a full-sized threat surrogate for use in training by surface and air ASW forces. The Chief of Naval Operations initiated the program in 2010 with the goal of achieving operational capability by late 2011. An engineering assessment of the MASTT reveales the surrogate cannot be used as a set-to-hit target for torpedo testing. After 5 years and an expenditure of approximately $15 Million, the Navy has started using the MASTT in limited search training. The Navy resisted design input from the operational test community and made it clear that the MASTT was not intended to support torpedo testing.

In support of a 2010 Urgent Operational Need Statement, the Navy funded the construction of the Steel Diesel-Electric Submarine (SSSK), a full-sized, moored, set-to-hit target consisting of an open steel framework with a series of corner reflectors to provide appropriate sonar highlights. This surrogate does provide a basic sonar signature. The Navy used the SSSK as a target for the MK 54 torpedo in a 2011 Quick Reaction Assessment and 2013 FOT&E. As part of the TEMP approval for the latter, DOT&E sent a memorandum indicating that the Navy must develop an appropriate mobile target to support future MK 54 testing.

Since early 2013, DOT&E has participated in a Navy working group attempting to define the requirements for a mobile set-to-hit torpedo target. The group has identified a spectrum of options and capabilities, ranging from a torpedo-sized vehicle towing a long acoustic array to a full-sized submarine surrogate. At the very least, the target is expected to be capable of mobile depth changes and high speeds, autonomous, and certified for representative lightweight torpedo set-to-hit scenarios. More advanced goals might include realistic active and passive sonar signatures to support ASW search, and reactive capability to present a more realistically evasive target. Cost estimates range from under $10 Million for a towed target to over $30 Million for a full-sized submarine simulator. The Navy has not funded the additional efforts.

Missile Warning and Infrared Countermeasure Test Capability Gaps

Aircraft Survivability Equipment (ASE) is an integral part of military fixed and rotary wing platforms to provide aircraft and crew protection, and is vital to mission effectiveness in hostile environments. DOT&E and TRMC co-lead the Infrared Countermeasure Test Resource Requirements Study (ITRRS), which is designed to identify shortfalls in infrared countermeasure (IRCM) testing and develop a prioritized investment roadmap of projects to mitigate current test gaps. However, the resultant roadmap is historically underfunded to a considerable degree. The roadmap has projects to address gaps for ground-based missile plume simulators, airborne missile plume simulators, hardware in the loop test facilities, installed system test facilities, surrogate threat missiles, instrumentation suites, open air test range improvements, and threat system acquisition and storage.

One of the high priority projects on the ITRRS list is the ability to measure threat signature data for the development or improvement of the threat models for heat seeking missiles and unguided hostile fire munitions used for the T&E of ASE. These models drive a large number of T&E simulation tools listed above. The DOT&E Center for Countermeasures serves as the executing activity for a TRMC Central T&E Investment Program (CTEIP) Resource Enhancement Project – the Joint Standard Instrumentation Suite (JSIS) – in order to mitigate this shortfall as well as provide ground truth for live missile firing and hostile fire tests of IRCM systems. When available, the JSIS initial operational capability (IOC) will support Advanced Threat Warner and Department of the Navy (DON) Large Aircraft Infrared Countermeasure (LAIRCM) operational testing. JSIS IOC capability is scheduled to be delivered in early FY17. JSIS can be deployed to static live fire venues outside the continental United States, where opportunities exist to measure and collect data for threat assets that are either not available, or of insufficient quantities domestically.

However, the JSIS IOC capability only partially addresses the needs identified by the ITRRS team. For example, it will not provide the capability to measure missile attitude information for the entire missile fly out, nor will the JSIS IOC capability meet all needs related to signature collection fidelity (i.e., frame rates and resolution). Full operational capability is required to meet the needs of the Army's Common Infrared Countermeasures (CIRCM) program, Navy's Advanced Threat Warner, Air Force's LAIRCM program, and the Naval Research Laboratory's Distributed Aperture Infrared Countermeasure (DAIRCM) program. JSIS full operational capability is also needed to collect signature data in support of T&E of advanced IRCM systems, currently in development, which operate in other wavelength bands. JSIS requires an additional investment of $43 Million to provide the full operational capability needed for IRCM T&E.

Both open-air test ranges and indoor test facilities require upgrades to test the latest missile warning systems and IRCM. The open-air test range improvements include additional firing points for multi-threat environments and angular separation, upgrades to improve test efficiency, improved instrumentation, and DAIRCM jitter and atmospheric distortion measurement capability. Hardware-in-the-loop and installed system test facilities are in need of upgrades to represent the latest threats in an operational simulated environment. Additionally, these facilities are heavily utilized and in need of expansion to meet program test schedules.

Threat Modeling and Simulation to Support Aircraft Survivability Equipment Testing

Acquiring actual threat systems for widespread testing is not always possible. To address this challenge, DOT&E funded standard, authoritative threat M&S for systems T&E. These may be coupled with U.S.-built threat representations. Although threat M&S capabilities have been used in T&E for many years, they were not always accurate representations, and different M&S instantiations of the same threats often produced different results. DOT&E's objective is to improve the fidelity and consistency of threat M&S at various T&E locations while reducing overall test costs.

Throughout the T&E process, M&S representations of threat systems can be used when actual threat components are not available. Use of these M&S representations may provide a more complete assessment of system operational performance than is possible using open-air facilities alone. M&S representations of threat systems also support testing when flight safety precludes live fire testing, such as missile launches against manned aircraft. For example, test programs may only conduct 10 – 20 live missile firings events; however, using a threat M&S test program may extend those results across a broader range of test conditions (typically 20,000) with different threats, ranges, altitudes, aspect angles, atmospheric conditions, and other environmental variables affecting weapon system performance.

DOT&E developed a T&E Threat M&S Configuration Management System to implement controls and distribution management for threat M&S to ensure integrity for realistic T&E and to ensure M&S consistency of test results among various T&E regimes. This system provides mechanisms to identify and correct anomalies between a threat and its M&S representations. It also assists in controlling model configuration changes, maintains critical documentation such as interface descriptions and validation documents, and provides updated threat M&S to multiple T&E facilities for developmental and operational test needs. The T&E Threat M&S Configuration Control Board (CCB), comprised of representatives from the T&E community and intelligence organizations, prioritizes existing threat M&S developments and changes to ensure updates are provided efficiently to T&E user facilities. Requests for T&E threat M&S, anomaly reports, and change requests are managed through an interface on DOD's Secret Internet Protocol Router Network. DOT&E is in the process of expanding the breadth of control by this CCB.

During FY16, the T&E Threat Resource Activity provided standardized authoritative threat M&S to multiple T&E facilities operated by the Army, Navy, and Air Force. The Services integrated and used this M&S to support ASE testing. DOT&E engaged the United States' closest allied nations to implement the same authoritative threat M&S for allied T&E. This allows the United States and its allies to use each other's ranges and facilities, leveraging this worldwide implementation for T&E.

DOT&E also developed and updated a threat M&S roadmap for ASE T&E to provide a comprehensive plan for future threat M&S. A good example is JSIS, which will capture threat data from live fire test events. The roadmap identifies projects to conduct systematic analyses of JSIS data to feed the development of threat-representative M&S to support U.S. and allied missile warning and infrared countermeasure systems.

DOT&E completed a threat radio-frequency (RF) M&S study which collected, analyzed, and presented information regarding the design, distribution, integration, and use of RF-related threat M&S across multiple organizations and the Services. The RF study provided a consolidated list of authoritative threat models developed by the Intelligence Production Centers (IPCs). The RF study team surveyed subject matter experts (SMEs) at the IPCs and T&E facilities to determine common issues with the implementation of M&S for T&E. The RF study provided the following list of recommendations to stakeholders for T&E M&S improvements:

1. Assist IPCs with RF threat M&S configuration management (CM) using the existing IR configuration management system
2. Maintain an up-to-date catalog of RF Threat M&S
3. Provide periodic RF threat M&S feedback between IPCs and T&E facilities
4. Sponsor and assist threat RF M&S hardware acceleration programs
5. Develop a roadmap for RF M&S threat representations and technology

DOT&E, in conjunction with TRMC, is developing a T&E threat M&S capability/investment roadmap. This comprehensive roadmap will address threat M&S investment needs to adequately evaluate airborne combat systems. The roadmap will also coordinate new development and sustainment programs to address EW test capability shortfalls. These new programs will require additional funding in the next five years.

Foreign Materiel Acquisition Support for T&E

DOT&E is responsible for ensuring U.S. weapons systems are tested in realistic threat environments, using actual threat systems to create these threat environments whenever possible and appropriate. DOT&E develops an annual prioritized list of foreign materiel required by upcoming operational tests. These requirements are submitted to the DIA Joint Foreign Materiel Program Office and are consolidated with Service requirements to drive Service and Intelligence Community collection opportunities. DOT&E coordinates with the Department of State to identify other opportunities to acquire foreign materiel for use in OT&E.

Foreign materiel requirements span all warfare areas, but DOT&E continues to place a priority on the acquisition of Man-Portable Air Defense Systems (MANPADS) to address significant threat shortfalls that affect testing for IRCM programs like CIRCM, LAIRCM, and DON LAIRCM. For some programs, a large quantity of MANPADS is required – for development of threat M&S, for use in hardware-in-the-loop laboratories, and for LFT&E, to present realistic threats to IRCM equipment. Using actual missiles and missile seekers aids evaluators in determining the effectiveness of IRCM equipment. During FY16, ongoing Foreign Materiel Acquisition efforts have continued to lead to new opportunities to acquire assets for IRCM equipment testing.

DOT&E's Test and Evaluation Threat Resource Activity (TETRA) – in collaboration with the Office of the Under Secretary of Defense for Intelligence and Department of State Weapons Removal and Abatement – has made significant progress in raising awareness of the critical shortfalls of MANPADS for T&E. TETRA briefed the National Security Council (NSC) Counter-Terrorism Task Force and the MANPADS Task Force. These efforts led to NSC tasking the organizations responsible for developing sources, which in turn led to the creation of more opportunities for acquisition to meet T&E requirements.

There is an extreme shortfall of foreign materiel for operational testing, particularly MANPADS and anti-tank guided missiles. This shortfall has become critical, as exemplified in the U.S. Special Oeprations Command's 2015 Joint Urgent Operational Needs Statement. Traditional sources have been fully consumed, and there is a critical need to identify and develop new sources and opportunities for acquiring foreign materiel. Foreign materiel acquisitions are usually very lengthy and unpredictable, making it difficult to identify appropriate year funding. DOT&E recommends adding a staff position within the Joint Foreign Materiel Program Office dedicated to developing and executing foreign materiel acquisition opportunities for operational testing. The funding requirement for this staff position is $300,000 per year. DOT&E also recommends a no-year or non-expiring funding line for foreign materiel acquisitions, funded at a level of $10 Million per year.

Tactical Engagement Simulation with Real-Time Casualty Assessment

Realistic operational environments and a well-equipped enemy intent on winning are fundamental to the adequate operational test of land and expeditionary combat systems. Force-on-force battles between tactical units represent the best method of creating a complex and evolving battlefield environment for testing and training. Simulated force-on-force battles must contain realism to cause commanders and Soldiers to make tactical decisions and react to the real-time conditions on the battlefield. Tactical Engagement Simulation with Real Time Casualty Assessment (TES/RTCA) systems integrate live, virtual, and constructive components to enable these simulated force-on-force battles, and provide a means for simulated engagements to have realistic outcomes based on the lethality and survivability characteristics of both the systems under test and the opposing threat systems. TES/RTCA systems must replicate the critical attributes of real-world combat environments, such as direct and indirect fires, IEDs and mines, and simulated battle damage and casualties. TES/RTCA systems must record the time-space position information and firing, damage, and casualty data for all players in the test event as an integrated part of the test control and data collection architecture. Post-test playback of these data provides a critical evaluation tool to determine the combat system's capability to support soldiers and marines as they conduct combat missions.

In FY15, the Army initiatied the Integrated Test Live, Virtual, and Constructive Environment (ITLE) project to address the known TES/RTCA capability shortfalls and future Army requirements. There was little progress made on the ITLE project in FY16; consequently, funding for the effort has been realigned. DOT&E is concerned that because of delays, ITLE may not be able to accomplish the TES/RTCA upgrades needed to support upcoming operational testing of the Army's major modernization programs.

The Marine Corps' current force-on-force training system, the Instrumented Tactical Engagement Simulation System II (ITESS II), does not support combat vehicle engagements. The Marine Corps Operational Test and Evaluation Activity had planned a substantial upgrade of ITESS II beginning in FY16 to support the upcoming operational testing of combat vehicles, but it was unable to secure the required funding. The estimated cost of the ITESS II upgrade was $9 Million.

DOT&E, beginning with its 2002 annual report, has emphasized the need for continued investment in TES/RTCA capabilities. Further, DOT&E requires these capabilities for testing systems such as Amphibious Combat Vehicle, Bradley and Abrams Upgrades, Armored Multi-purpose Vehicle, AH-64E Block III, Joint Light Tactical Vehicle, and Stryker Upgrades.

Warrior Injury Assessment Manikin

DOT&E has been the advocate for an Army-led project to enhance the Department's ability to assess injuries from under-vehicle IED and mine blasts by creating a military-specific anthropomorphic test device (ATD) and associated injury criteria tailored to the underbody blast environment. The need for this was first documented in 2009 as a result of a SECDEF-directed evaluation of the Department's underbody blast modeling and simulation capabilities, and the need has been validated repeatedly since then. The evaluation concluded that automotive crash test dummies used in LFT&E and the consequent injury criteria – designed and developed for forces and accelerations in the horizontal plane, as seen in automotive frontal impact-induced injuries – were not adequate to assess the effects of the forces and accelerations in the vertical plane typically seen in combat-induced unerbody blast events. To address this limitation in 2010, DOT&E championed initial funding for the Army to lead the effort that became known as the Warrior Injury Assessment Manikin (WIAMan) project. Under this project, the Army initiated critical biomechanical research and the anthropomorphic test devices (ATD) development program to increase DOD's understanding of the cause and nature of injuries incurred in underbody blast combat events.

The science and technology (S&T) and ATD development aspects of the project are being executed by the Army Research Laboratory's WIAMan Engineering Office (WEO). In 2015, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) determined that the WIAMan project is an Acquisiton Category II program of record and, as such, ASA(ALT) has determined that the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) will be responsible for the project's execution post Milestone B. The WEO continues to accomplish its technical goals for S&T and ATD development research, but as a result of the acquisition approach, the WEO is now also supporting PEO STRI, as required by a memorandum of agreement signed by the Army Research, Development, and Engineering Command and PEO STRI. However, no additional personnel or funding has been procured for the WEO to address these additional duties. This has the potential to tax the resources of the WEO and shift the emphasis of the subject matter experts within WEO from S&T to acquisition. The planning and execution of the formal acquisition process is behind schedule, while incurring significant overhead costs.

In FY15, the Assistant Secretary of Defense for Health Affairs committed S&T funding for the program post Milestone B to ensure critical injury biomechanics research is completed. However, the Army had not provided a similar committment to fund this program's acquisition. Consequently, in FY15, DOT&E supported fully funding the acquisition side of the project. As a result, the Army was directed to allocate $16.2 Million over FY17 and FY18 "to continue RDT&E activities and further the acquisition process." However, the critical funding required to continue and complete the execution of this program past FY18 has not yet been resolved.

Some within the Army have questioned whether DOD still needs a combat-specific injury assessment capability. In the view of DOT&E, it is entirely appropriate for DOD, and in particular for the Army, to accord the same high priority to testing and verifying the protection provided to soldiers by their combat vehicles that the commercial automotive industry accords to testing and verifying the protection provided to the U.S. public by their automobiles.

Testing in Urban Environments

Operations in urban environments present unique challenges to the military Services and their equipment. Degraded mobility, maneuver, communications, and situational awareness; a large civilian presence; the risk of collateral damage; reduced stand-off distances; and unique threat profiles are some of the conditions present during urban operations. These challenges – and a world population that is becoming increasingly urban – reinforce the requirement that systems be tested in realistic urban environments. DOT&E, beginning with its 2002 annual report, has been highlighting the need for larger and more complex urban test environments.

With the cancellation of the Army's Joint Urban Test Capability in 2015, the long-standing urban environment operational and developmental test capability shortfall is not being addressed. DOT&E recommends that the Army revisit the urban test capability requirement to capture current and future T&E requirements, and develop a new approach to addressing this shortfall.

Biological Defense Testing at West Desert Test Center
In late FY15, DOD suspended the production of and testing with biological select agents and toxins (BSAT) and derivatives of BSAT materials at the West Desert Test Center (WDTC) on Dugway Proving Ground, Utah. On October 16, 2015, the Secretary of the Army approved the reassignment of the WDTC Life Science Division to the Edgewood Chemical Biological Center (ECBC) in Edgewood, Maryland. On July 1, 2016, ECBC took control of the Life Science Division and changed its name to the WDTC Biological Testing Branch (BTB). In August 2016, the Army completed a review of safety and surety protocols and procedures at WDTC and approved the resumption of field test activities using biological simulants that are safe for open-air use. The Army requested a withdrawal of the Dugway Proving Ground Biosafety Level Three (BSL 3) Centers for Disease Control and Prevention (CDC) permits and plans to apply for a new BSL 3 CDC permit for WDTC BTB facilities. The Army's current projection for achieving WDTC BTB BSL-3 certification is late 2019. WDTC and the BTB have unique biological testing facilities and capabilities that are essential to operationally realistic T&E of biological defense systems. DOT&E continues to monitor the requirement for BSL-3 and work with the Army to develop mitigation plans until the full biological test capability comes back online.

Range Sustainability and Radio Frequency Spectrum
Adequate land-, air-, and sea-space are critical for DOD's capability to test weapon and associated systems in operationally realistic conditions under which performance data can be collected, public safety can be ensured, and physical security and cybersecurity can be protected. Range sustainability is the preservation of, and advocacy for, those spaces. Sustainability is challenged by encroachment factors such as incompatible infrastructure, urban development, natural resource constraints, and frequency spectrum losses. Each of these factors may limit the use of land-, air-, and sea-space for DOT&E to execute its operational test and evaluation mission.

Despite DOT&E's best efforts there are a number of continuing challenges to both preserving current test capabilities and ensuring that there are avenues available to support testing of future weapon systems. Future testing will require expanded footprints, networked sensors, and advanced range capabilities which address complex cybersecurity environments.

Two primary strategies are essential to protect range space and test capabilities. The first is data-driven compatibility analysis – based on weapon system performance requirements – to ensure that evaluations conducted are credible. The second is outreach to other Federal agencies, state and local governments, and non-governmental organizations, to address issues early and to develop solutions that benefit all participants.

A recurrent theme in the evaluations performed for range sustainability is that while most of the challenges have either no compatibility risks or have risks that can be mitigated, there are a few cases that do have adverse impacts on test capabilities. Ongoing vigilance is required to ensure that DOT&E knows about projects that may pose risks to operational testing capabilities, now and in the future, and that DOT&E is in a position to mitigate risks early in the review cycle.

Current major areas of concern are:
- Energy infrastructure projects
- Natural resource protections
- National monuments and marine sanctuaries
- Frequency spectrum reallocation
- Foreign investment
- Privately owned and operated drones

Energy infrastructure projects can adversely affect instrumentation essential for obtaining data on weapon systems being tested, and can create physical obstructions that limit the use of test space. Under the provisions of Public Law 111 383, Section 358, as amended by Public Law 112 81, Section 331, DOD conducts compatibility evaluations of energy infrastructure to ensure that adverse impacts to national security can be identified and mitigated. DOT&E is an active participant in the DOD process to ensure that test capabilities required for realistic testing of current and future weapon systems are available for use. The process enables review and approval or disapproval of projects based upon risk to operational test capabilities. However, the tools available to the Department to require mitigation of problematic aspects of proposed energy infrastructure projects are not currently sufficient to prevent all adverse impacts to test capabilities. The DoD can only directly control development on DOD owned, leased, or withdrawn property. In all other circumstances, the Department must rely on a mix of authorities available to other Federal agencies, or to state and local government intervention. Yet these authorities have proven to be problematic in certain instances. For example:
- DOD relies on the FAA obstruction to flight notification requirements in section 44718 of title 49, U.S. Code (49 USC 44718), to receive notification of energy infrastructure projects. However, the statute gives DOD no authority to evaluate structures not covered by 49 USC 44718, nor does it prescribe any mechanism for DOD to ensure that unacceptable risks do not occur. The FAA does not currently have the authority to withhold approval for projects that do not pose a hazard to flight safety, but are objectionable to DOD. DOT&E has been researching options by which DOD can object to renewable energy and associated infrastructure projects on the basis of adverse impact to national security and will continue to explore and shape policies and procedures that can be

used to ensure that required operational test capabilities are available for use.

- Developers proposing energy infrastructure projects on Federal land must go through the National Environmental Protection Act (NEPA) process. While DOD can be a participating agency on those projects which have the potential to constrain the conduct of operational testing, current rules do not allow the Department to object to projects that would impact its ability to satisfy reasonably foreseeable future testing requirements; the processes are focused on consideration of documented requirements. As mentioned earlier in this report, the Department is confident that the expanded capabilities of new weapon systems will drive operational testing requirements for test spaces with larger footprints than are currently available. DOT&E will work with Federal agencies to ensure that NEPA procedures provide for consideration of reasonable and foreseeable actions to support mid- and long-term weapon systems test requirements.
- For many of the test ranges, particularly those in the Southwest, Federal land is withdrawn for specified periods of time. DOT&E conducts test missions using airspace that is restricted as regulatory, special use airspace through the FAA, and sea-space that is designated as non-regulatory, special use air-space by the FAA. For land withdrawal extensions, test ranges prepare range planning documents to support continued withdrawal. These plans integrate planned test requirements for the individual test range; however they may not adequately consider requirements for integrating requirements with those of other test ranges to allow for combined land and air resources to support future tests of longer range and networked weapon systems. DOT&E will investigate mechanisms to provide for sufficient air- and land-space to support this expanded envelope testing.

The Department requires that its weapon systems be capable of operating in a wide variety of environments, and its ranges are designed to allow testing and training across these environments. However, DOD ranges contain environmentally sensitive flora and fauna, including those that migrate from external disturbed areas. The U. S. Fish and Wildlife Service list of threatened and endangered species and Reports to Congress on the Recovery of Threatened and Endangered Species indicate that the total number of U.S. plant and animal species that are identified as threatened or endangered has more than doubled from 581 in 1990 to 1604 as of September 2016. The growing list of threatened and endangered species, and their proximity to DOD ranges, places significant pressure on the Department to safeguard areas where protected species and habitat exist while testing weapons systems in operationally realistic environments. The DOD challenge is to integrate weapons systems testing needs with environmental restrictions that prevent use of areas designated for operational testing. Accordingly, DOT&E will actively engage other Federal, state, local, and private organizations to reach mutually agreeable arrangements on means to accommodate test disturbances while conserving natural resources.

The declaration of a new or expanded national monument and marine sanctuary has the potential to encroach on existing test ranges, or to preclude expansion of ranges in the future. The challenge is to allow for testing activities, which require vehicle and personnel transit on or above these areas and which may result in damage from test objects, while preserving natural resources. To ensure that use of these areas to satisfy national security requirements, to include test and evaluation, is not precluded, it is essential that the proclamations establishing national monuments and marine sanctuaries include specific language permitting continued DOD use.

Frequency spectrum is required to conduct test operations, and is vital for controlling autonomous vehicles, sending and receiving test data, and ensuring range safety. However, there are continuing pressures to repurpose spectrum currently allocated to DoD to support national broadband expansion. The challenge is how to accommodate approved spectrum repurposing while retaining required spectrum for use by DoD when it is needed. The strategies employed include working to preserve essential frequency spectrum currently available for DoD use and supporting research initiatives for technologies and equipment that makes the most efficient use of available spectrum. DOT&E will continue to monitor frequency spectrum issues related to operational test requirements, review policies and procedures ensuing from DoD's Spectrum Strategy, and engage in other issues that may adversely impact use of spectrum for T&E.

Foreign investment in resources and facilities proximate to test ranges may create undesirable opportunities for intelligence gathering on weapons capabilities. Foreign purchases of U.S. companies that provide test and telemetry equipment used on our ranges and test facilities may likewise create operational security challenges. DOT&E reviews projects referred by the Committee on Foreign Investment in the United States (CFIUS) for possible security risks for foreign data collection. During the past twelve months, 207 cases – with more than 3,500 supporting documents – were reviewed. Sixteen cases were assessed to pose a potential threat to test or training ranges and required further investigation and development of mitigation strategies. However, as currently constituted, CFIUS provides only for the review of projects voluntarily submitted by applicants; there is a potential risk that other, unrecorded transactions may create operational security vulnerabilities. DOT&E will exercise vigilance in this area to ensure that data from weapon system tests are not compromised.

The advent of inexpensive drones, and the institution of public licensure policies, creates potential risks from drones intruding into sensitive DoD airspace, either inadvertently or with malicious intent. This creates safety of flight dangers, and opens potential adversaries to collect information on weapons characteristics. At present, DoD has very few legal avenues to prevent such intrusions, or to act when intrusions are detected. DOT&E will actively work within the Department and with other Federal agencies to ensure that adequate procedures are in place to ensure that drones do not create impediments to effective operational testing.

Joint Test and Evaluation

Joint Test and Evaluation

Joint Test and Evaluation (JT&E)

The primary objective of the Joint Test and Evaluation (JT&E) Program is to rapidly provide non-materiel solutions to operational deficiencies identified by the joint military community. The program achieves this objective by developing new tactics, techniques, and procedures (TTP) and rigorously measuring the extent to which their use improves operational outcomes. JT&E projects may develop products that have implications beyond TTP. Sponsoring organizations submit these products to the appropriate Service or Combatant Command as doctrine change requests. Products from JT&E projects have been incorporated into joint and multi Service documents through the Joint Requirements Oversight Council process, Joint Staff doctrine updates, Service training centers, and through coordination with the Air Land Sea Application Center. The JT&E Program also develops operational testing methods that have joint application. The program is complementary to, but not part of, the acquisition process.

The JT&E Program has two test methods available for customers: the Joint Test and the Quick Reaction Test (QRT). Additionally, a Special Project is available for command directed or customer funded test projects.

The Joint Test is, on average, a two-year project, preceded by a six-month Joint Feasibility Study. A Joint Test involves an in-depth, methodical test and evaluation of issues and seeks to identify their solutions. DOT&E funds the sponsor-led test team, which provides the customer periodic feedback and useable, interim test products. The JT&E Program charters two new Joint Tests annually. The JT&E Program managed seven Joint Tests in FY16 that focused on the needs of operational forces. Projects annotated with an asterisk (*) were completed in FY16:

- Digitally Aided Close Air Support (DACAS)
- Four Pillars of Integrated Air and Missile Defense (4-PI)*
- Joint Advanced Zensor to Zhooter (JAZZ)
- Joint-Base Architecture for Secure Industrial Control Systems (J-BASICS)*
- Joint-Fiber Laser Mission Engagement (J-FLaME)*
- Joint Pre-/Post-Attack Operations Supporting Survivability And Endurability (J-POSSE)
- Joint Tactical Air Picture (JTAP)*

QRTs are intended to solve urgent issues in less than a year. The program managed 18 QRTs in FY16:

- Civil Military Engagement Development-Joint Targeting/Non-Lethal (CMED-JT/NL)*
- Cyber Degraded Training (CDT)
- Homeland Underwater Port Assessment Plan (HUPAP)
- Joint Accelerated Collaborative Targeting (J-ACT)
- Joint Air Operations Center Command and Control in a Contested Degraded Environment (JADC)
- Joint Biological/Radiological Mortuary Affairs Contaminated Remains Mitigation Site (JBRM)*
- Joint-Cyber Synchronization into Air Tasking Order (J-CAT)*
- Joint Cyber Integration of DOD Information Network Operations (J-CID)
- Joint Intelligence Surveillance and Reconnaissance in a Contested Area (JICA)*
- Joint Interagency-Cyber Enhanced Detection and Monitoring (JI-CEDM)
- Joint Laser Anti-Satellite Mitigation Mission Planning (J-LAMMP)*
- Joint Personnel Recovery Information Digital Exchange (J-PRIDE)
- Joint Sniper Performance Improvement Methodology (JSniPIM)*
- Joint Talon Thresher Theater Integration (JT3I)
- Joint Target Development: Target System Analysis Standards and Procedures (T-SaP)*
- Joint Unmanned Aerial Vehicle Swarming Integration (JUSI)*
- Theater Joint Land Forces Component Commander Common Operational Picture (T-COP)*
- Optimization of Social Media and Open Source Information Support (OSMOSIS)

As directed by DOT&E, the program executes Special Projects that address DOD-wide problems. Special Projects generally address emergent issues that are not addressed by any other DOD agency, but that need a rigorously tested solution. The program managed two Special Projects in FY16:

- Joint and Community Attributes-Based Access Control Authorization for Transportation Services (J-CAATS)*
- Joint National Capital Region Enhanced Surveillance Tactics, Techniques, and Procedures (J-NEST)

JOINT TESTS

DIGITALLY AIDED CLOSE AIR SUPPORT (DACAS)

Sponsor/Start Date: Joint Staff J6/February 2016

Purpose: To develop, test, and evaluate standardized TTP so Joint Terminal Attack Controllers (JTAC), Joint Fires Observers (JFO), and Close Air Support (CAS) aircrew can realize the advantage of DACAS capabilities, including shared situational awareness, increased confidence prior to weapons release, and improved kill chain timeliness.

Products/Benefits:

- Enable JTAC and aircrew to access existing networks and exploit DACAS benefits
- Decrease human input error through machine-to-machine data exchange
- Instill confidence prior to weapons release

FOUR PILLARS OF INTEGRATED AIR AND MISSILE DEFENSE (4-PI)
(CLOSED AUGUST 2016)

Sponsor/Start Date: U.S. European Command (USEUCOM), U.S. Army Space and Missile Defense Command, and U.S. Air Forces Europe-Air Forces Africa/August 2014

Purpose: To develop and test TTP that enable sharing of existing sensor data to enhance the concurrent execution of integrated air and missile defense (IAMD) active defenses, passive defenses, attack operations, and battle management command, control, communications, and intelligence (BMC3I) in response to ballistic missile attacks across Combatant Command areas of responsibility (AOR) in a coalition environment.

Products/Benefits:

- TTP on sharing data to support concurrent offensive and defensive counter-air operations in order to better defend against, and mitigate the effects of, a ballistic missile attack across Combatant Command boundaries with coalition partners (USEUCOM, U.S. Central Command (USCENTCOM) and NATO)
- Enabled cross-AOR data sharing of Joint Automated Deep Operations Coordination System information, which allows communication of USEUCOM priorities and real-time engagement monitoring and established persistent capability that can be easily turned on when operational need arises
- Developed cross-AOR attack operations Joint Planning Team construct and Collaborative Planning Environment TTP, which serves as a baseline for Joint Staff cross-AOR planning orders to resolve potential cross-AOR gaps and seams
- Standardized BMC3I capabilities and Global Command and Control System – Joint configurations to maximize efficiencies, support command and control collaboration, and enable sharing of IAMD sensor data
- Enhanced civil-military passive defense/missile warning process for NATO nations, extensible to other Shared Early Warning System partners

JOINT ADVANCED ZENSOR-TO-ZHOOTER (JAZZ)

Sponsor/Start Date: U.S. Pacific Command (USPACOM)/ August 2015

Purpose: To develop, evaluate, and validate TTP to more efficiently and effectively gain and maintain battlespace awareness through integration of rapidly developed capabilities to support combat operations in anti-access/area denial environments.

Products/Benefits:

- A sensor to shooter TTP that enables sharing of advanced sensor and National-Tactical Integration (NTI) data between 5th and 4th generation fighters, resulting in increased situational awareness, improved engagement opportunities, and better utilization of weapon systems
- Documented roles and responsibilities for the Operational Air Component Commander and the tactical datalink network designers to plan and execute integration of advanced sensors and NTI into any theater of operations

JOINT-BASE ARCHITECTURE FOR SECURE INDUSTRIAL CONTROL SYSTEMS (J-BASICS)
(CLOSED DECEMBER 2015)

Sponsor/Start Date: U.S. Cyber Command (USCYBERCOM)/ February 2014

Purpose: To develop, test, and evaluate Advanced Cyber Industrial Control System (ACI) TTP to improve the ability of industrial control system (ICS) network managers to detect, mitigate, and recover from nation-state cyber-attacks.

Products/Benefits: ACI TTP and related ICS network manager training packages provided the following capabilities:

- Resiliency to DOD ICS networks and IT infrastructures
- Increased Command confidence resulting from the ACI TTP, for ICS network managers to: detect nation-state presence in DOD ICS networks, mitigate damage to underlying processes supported by the ICS in the event of a cyber-attack, and quickly recover the ICS network to be mission capable
- Policy and implementation guidance recommendations for ICS network security to Commander, USCYBERCOM and the Assistant Secretary of Defense, Energy, Installations and Environment
- Training package and cyber exercise scenarios that provide ICS operators an understanding of the TTP and its practical application

JOINT-FIBER LASER MISSION ENGAGEMENT (J-FLAME)
(CLOSED AUGUST 2016)

Sponsor/Start Date: Naval Surface Warfare Center, Dahlgren Division/August 2014

Purpose: To develop and test TTP that integrate emerging directed energy laser (DEL) capabilities into joint fires and force protection missions.

Products/Benefits: Improved DEL Operations in the Joint Battlespace:

- Integrated DEL systems into joint fires planning and execution, focusing on actions required for deconfliction, integration, synchronization, and safety of these systems in a complex and congested battlespace

- Addressed force protection mission requirement against asymmetric threats (unmanned aerial systems and small boats), focusing on unique aspects of DELs that impact the joint battlespace (for example, new coordinating measures, Laser Engagement Zones, and Laser Operating Areas) that personnel at both operational and tactical levels need to consider
- Provided laser dwell time versus range graphs for various DEL power classes and mission sets to assist operators to effectively and efficiently employ DELs
- Provided information on risks associated with DEL reflected energy and risk estimate distances for use in minimizing risks to friendly troops in close proximity to DEL targets
- Provided recommendations to assist the Services in DEL system development and acquisition, as well as with integrating DELs into the battlespace common operational picture

JOINT PRE-/POST-ATTACK OPERATIONS SUPPORTING SURVIVABILITY AND ENDURABILITY (J-POSSE)

Sponsor/Start Date: U. S. Strategic Command (USSTRATCOM)/February 2015

Purpose: To develop, test, and evaluate TTP to provide joint operators the ability to survive an electromagnetic pulse (EMP) event in order to ensure continuous mission functionality.

Products/Benefits:
- Standardized procedures that provide overarching guidance for required actions before and after an EMP event in order to survive it
- Results inform future resourcing decisions regarding physical enhancements
- Extensible to other mission systems potentially vulnerable to EMP effects

JOINT TACTICAL AIR PICTURE (JTAP)
(CLOSED FEBRUARY 2016)

Sponsor/Start Date: USPACOM/February 2014

Purpose: To develop, evaluate, and validate TTP to improve the joint air picture and engagement opportunities, which decrease the risks of preemptive hostile attack and fratricide.

Products/Benefits:
- Developed TTP to reduce radio frequency network loading by moving participants to internet protocol architectures resulting in a greater number of timeslots available for participants
- Developed Multi-Service IAMD TTP to enhance integrated fire control/between ground sensors and air shooters for defensive counter-air engagements thereby increasing the number of available tracks containing fire control quality data

---

QUICK REACTION TESTS

CIVIL MILITARY ENGAGEMENT DEVELOPMENT-JOINT TARGETING/NON-LETHAL (CMED-JT/NL)
(CLOSED MAY 2016)

Sponsor/Start Date: U.S. Army Civil Affairs & Psychological Operations Command (Airborne)/February 2015

Purpose: To develop, test, and validate civil-military engagement development (CMED) TTP to improve the non-lethal aspects of the joint targeting process. To increase the Combatant Command staff's ability to integrate civil information and analysis products into the joint targeting cycle and improve basic, intermediate, and advanced joint target folder development, entity-level development, prioritization (phase two of the joint targeting process), and no strike and restricted target lists.

Products/Benefits:
The CMED-JT/NL-developed TTP provided Commanders the ability to integrate civil military information into phase two of the joint targeting process.

CYBER-DEGRADED TRAINING (CDT)

Sponsor/Start Date: USPACOM/Feb 2016

Purpose: To develop, test, and evaluate concept of operations (CONOPS) and TTP that will address the characteristics of cyber-degraded training environments as well as how to select, employ, and overcome these capabilities relative to factors such as military training objectives, Commander's risk tolerance, threat representation, and exercise complexity

Products/Benefits: TTP & CONOPS
- TTP and CONOPS that provide USPACOM with standardized, comprehensive tools to support Commanders at all levels with the ability to function in a cyber-degraded environment
- CONOPS identifies the different types of degraded cyber environments that can be created and options of how trainers, planners, and subject matter experts can employ them for training and exercise activities

HOMELAND UNDERWATER PORT ASSESSMENT PLAN (HUPAP)

Sponsor/Start Date: North American Aerospace Defense Command (NORAD)-U.S. Northern Command (USNORTHCOM)/June 2015

Purpose: To develop and evaluate TTP for underwater port assessments to include specific details about the roles and responsibilities of the stakeholders; identify available local, state, and federal force multipliers; provide data collection, compilation, and sharing guidance; and identify gaps in response considerations.

Products/Benefits:
- Comprehensive TTP that prescribes the standards and activities necessary to gather interagency underwater port

information for homeland ports and internal waterways in preparation for a catastrophic event
- Assists port authorities when developing an Interagency Underwater Port Assessment that will provide DOD and interagency partners with preparation, response, and recovery information necessary to reopen ports and waterways

JOINT ACCELERATED COLLABORATIVE TARGETING (J-ACT)

Sponsor/Start Date: USSTRATCOM/February 2016

Purpose: To develop and assess a CONOPS that uses an accelerated intelligence processing, exploitation, and dissemination (PED) process that streamlines intelligence analysis and coordination with targeteers to increase the speed of potential target object classification and verification.

Products/Benefits:
- A PED CONOPS that accelerates imagery analysis, target object classification, and target verification.

JOINT AIR OPERATIONS CENTER (AOC) COMMAND AND CONTROL (C2) IN A CONTESTED DEGRADED ENVIRONMENT (JADC)

Sponsor/Start Date: USPACOM/February 2016

Purpose: To develop TTP to support joint AOC distributed planning, execution, and assessment in a contested, degraded, and operationally limited environment by distributing authorities and effectively employing airpower and supporting forces.

Products/Benefits:
- TTP that enables delegation of operational airpower C2 from the joint AOC to subordinate Commanders
- Delegation of authorities that empower leaders at lower echelons of command to continue execution of the Commander's intent with limited loss of operational or tactical initiative

JOINT BIOLOGICAL/RADIOLOGICAL MORTUARY AFFAIRS CONTAMINATED REMAINS MITIGATION SITE (JBRM) (CLOSED SEPTEMBER 2016)

Sponsor/Start Date: U.S. Army Quartermaster School/June 2015

Purpose: To develop TTP for the safe processing, identification, and preparation for evacuation of biologically or radiologically contaminated human remains. To improve the Mortuary Affairs Contaminated Remains Mitigation Site effectiveness and safety for operational mission requirements, including hazard mitigation, preserving forensic evidence, establishing chain of custody, supporting positive identification processes, and preparing remains for evacuation.

Products/Benefits:
- Updates to Army and joint doctrine, with primary focus on Army Techniques Publication 4-46.2, Mortuary Affairs Contaminated Remains Mitigation Site Operations, as related to biological or radiological contaminated human remains
- Verified data and tools to the mortuary affairs community for use in both USNORTHCOM homeland defense missions and DOD's worldwide contingency operations
- Creation of the Mortuary Affairs Contaminated Remains Mitigation Site Tactical Handbook

JOINT-CYBER SYNCHRONIZATION INTO AIR TASKING ORDER (J-CAT) (CLOSED FEBRUARY 2016)

Sponsor/Start Date: USPACOM/October 2014

Purpose: To develop TTP for Combatant Commands to direct regionally synchronized and globally deconflicted cyber fires and integrate offensive cyberspace operations into air tasking order development and execution processes to synchronize cyber operations with other joint fires and provide coordination and deconfliction of global cyber operations with USCYBERCOM's cyberspace tasking order.

Products/Benefits: An operational TTP for incorporation of cyber fires and effects into the Combatant Command's air tasking order and USCYBERCOM's cyberspace tasking order.

JOINT CYBER INTEGRATION OF DOD INFORMATION NETWORK OPERATIONS (J-CID)

Sponsor/Start Date: USPACOM/June 2015

Purpose: To develop a CONOPS and TTP for the Combatant Commands' Joint Cyber Centers that fully integrates the organization, authorities, and capabilities of DOD Information Network commands in support of joint theater cyber operations.

Products/Benefits: CONOPS and TTP that provide best practices for the support of regional operations, situational understanding, and decision making for cyberspace operations between regional DOD Information Network commands and Joint Cyber Centers.

JOINT INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE IN A CONTESTED AREA (JICA) (CLOSED FEBRUARY 2016)

Sponsor/Start Date: 25th Air Force/October 2014

Purpose: To develop TTP that improve information flow from national intelligence, surveillance, and reconnaissance (ISR) capabilities to operational and tactical-level users in an anti-access/area denial environment.

Products/Benefits: TTP that establish a 'trigger' for AOC intelligence personnel to request ISR support from national assets by defining and identifying the level of degradation impairing organic theater and tactical ISR capabilities and instructions on how to efficiently request ISR support.

JOINT INTERAGENCY-CYBER ENHANCED DETECTION AND MONITORING (JI-CEDM)

Sponsor/Start Date: Joint Interagency Task Force South (JIATFS)/June 2016

Purpose: To develop TTP to coordinate and utilize interagency cyber domain support from DOD, law enforcement, and intelligence community partners in the conduct of detection and monitoring (D&M) missions.

Products/Benefits: CONOPS and TTP for the timely and efficient use of internal and external cyber resources to support JIATFS requirements, eliminate redundancy, and maximize the impact of cyber domain information in conducting D&M operations

JOINT LASER ANTI-SATELLITE MITIGATION MISSION PLANNING (J-LAMMP)
(CLOSED OCTOBER 2015)

Sponsor/Start Date: U.S. Air Force Warfare Center/June 2014

Purpose: To develop TTP to quantify the anti-satellite (ASAT) risk to low-earth and highly elliptical orbit satellites using optical systems and requiring operational and tactical methods to mitigate existing low-power laser threats. The TTP incorporates payload susceptibility information into mission planning to mitigate laser ASAT threats at both the operational and tactical levels of space operations.

Products/Benefits:
- Ability to incorporate payload susceptibility information into the mission planning processes at operational and tactical levels in response to laser ASAT threats
- Formalized established communications processes within the Joint Space Operations Center (JSpOC) and between the JSpOC and subordinate units

JOINT PERSONNEL RECOVERY INFORMATION DIGITAL EXCHANGE (J-PRIDE)
(CLOSED OCTOBER 2016)

Sponsor/Start Date: Joint Staff J7/June 2015

Purpose: To develop TTP to pass critical information across existing hybrid networks between isolated personnel, recovery forces, and command and control nodes during joint personnel recovery (PR) missions.

Products/Benefits:
- Formalized mission critical information across operational and tactical PR nodes to enhance mission effectiveness and increase survivability
- Provided a standardized 15-line PR message format across joint forces

JOINT SNIPER PERFORMANCE IMPROVEMENT METHODOLOGY (JSNIPIM)
(CLOSED JANUARY 2016)

Sponsor/Start Date: U.S. Marine Corps Weapons Training Battalion/October 2014

Purpose: To develop TTP and training methodologies to improve sniper teams' ability to identify, range, lead, and engage human motion-type moving targets at distances of 300 to 1,000 meters at speeds of up to 10 miles per hour.

Products/Benefits: Developed a sniper-carried memory aid and a training support package with learning objectives, an instructor guide, and student handouts that:

- Enable instructors to teach, test, and qualify students on engaging moving targets at distances of 300 to 1,000 meters at speeds of up to 10 miles per hour
- Update curriculums for all DOD sniper schools

JOINT TALON THRESHER THEATER INTEGRATION (JT3I)

Sponsor/Start Date: USPACOM/October 2015

Purpose: To develop a CONOPS that clearly defines the optimal operating parameters of the Talon THRESHER system and standardizes user operating procedures to enhance air domain awareness within theater command and control nodes, joint AOCs, and national-tactical integration cells.

Products/Benefits:
- Standardized operating parameters and procedures to utilize and disseminate Talon THRESHER data
- Enhanced analysis of air track patterns of behavior
- Timely output of correlated air picture in multiple security formats

JOINT TARGET DEVELOPMENT: TARGET SYSTEM ANALYSIS STANDARDS AND PROCEDURES (T-SAP)
(CLOSED MAY 2016)

Sponsor/Start Date: Joint Staff J2/February 2015

Purpose: To develop TTP for targeteers and intelligence analysts to conduct target system analysis (TSA) for joint force operations and to standardize and enhance federated TSA production in support of deliberate and crisis action planning.

Products/Benefits:
- TSA TTP to support joint force planning and update Chairman of the Joint Chiefs of Staff Instruction 3370.01, Target Development Standards
- Provided applicable doctrine change recommendations that will be transitioned to the Joint Staff J2

JOINT UNMANNED AERIAL VEHICLE SWARMING INTEGRATION (JUSI)
(CLOSED JULY 2016)

Sponsor/Start Date: USPACOM/February 2015

Purpose: To develop, test, and validate a concept of employment that addresses operational use of swarming unmanned aircraft (UA) carrying electronic attack (EA) payloads against an advanced integrated air defense system (IADS) in an anti-access/area denial environment.

Products/Benefits:
- A concept of employment for UA swarms performing stand-in EA to degrade and deny the hostile IADS kill chain in support of joint air vehicles
- Identified capabilities and limitations of existing planning and modeling and simulation tools for this mission

THEATER JOINT LAND FORCES COMPONENT COMMANDER COMMON OPERATIONAL PICTURE (T-COP)
(CLOSED JUNE 2016)

Sponsor/Start Date: USPACOM/February 2015

Purpose: To develop a TTP and handbook for the USPACOM land forces common operating picture (COP) system to streamline the integration of participating units and various systems into the existing land domain COP.

Products/Benefits:
- Joint TTP that is extensible to other Combatant Commands seeking to enhance or develop similar land domain COPs for their specific needs
- A common processes handbook to effectively maintain the COP and document Service specific practices

OPTIMIZATION OF SOCIAL MEDIA AND OPEN SOURCE INFORMATION SUPPORT QRT (OSMOSIS)

Sponsor/Start Date: USCENTCOM/May 2016

Purpose: To develop TTP to rapidly and effectively gain near-real-time situational awareness using published digital media (new and traditional media sources) available on a global basis to enhance decision-making, planning, and execution of the Civil Affairs, Psychological Operations/Military Information and Support Operations, and Public Affairs missions.

Products/Benefits:
- Improved information gathering from traditional and non-traditional sources to provide the data necessary to create value focused, fused information for analysis to enhance the situational awareness of Commanders at the tactical, operational, and strategic levels.
- Accelerate employment of the Information Volume and Velocity application, a data extraction and aggregation application, across a broad set of missions such as: Defense support of civil authorities, humanitarian aid/disaster relief, strategic communications, counterterrorism, stability and counterinsurgency operations, joint interdiction operations, and peace operations

SPECIAL PROJECTS

JOINT AND COMMUNITY ATTRIBUTES-BASED ACCESS CONTROL AUTHORIZATION FOR TRANSPORTATION SERVICES (J-CAATS)
(CLOSED JULY 2016)

Sponsor/Start Date: U.S. Transportation Command/February 2015

Purpose: To develop TTP and CONOPS for providing secure, yet timely and appropriate, data access for DOD users using an attributes-based access control approach.

Products/Benefits:
- TTP that detailed the technical parameters and provided step-by-step guidance regarding the installation and use of the J-CAATS capability
- CONOPS that describes the overall planning, resources, and timelines required to proceed with usage

JOINT NATIONAL CAPITAL REGION ENHANCED SURVEILLANCE TACTICS, TECHNIQUES, AND PROCEDURES (J-NEST)

Sponsor/Start Date: NORAD/October 2014

Purpose: To develop TTP to incorporate emerging sensor capabilities into the NORAD and USNORTHCOM family of systems to support the air defense mission.

Products/Benefits:
- TTP that enable tactical, operational, and strategic command and control nodes to more fully employ the expanded detection, improved identification, and enhanced engagement of cruise missile threats to the national capital region
- TTP on utilization of advanced equipment capabilities to execute an effective joint engagement sequence for cruise missile defense

Center for Countermeasures

Center for Countermeasures

The Center for Countermeasures (CCM)

The Center for Countermeasures (the Center) is a joint activity that directs, coordinates, supports, and conducts independent countermeasure/counter-countermeasure (CM/CCM) T&E activities of U.S. and foreign weapons systems, subsystems, sensors, and related components. The Center accomplishes this work in support of DOT&E, the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation ((DASD(DT&E)), weapon systems developers, and the Services. The Center's testing and analyses directly support evaluations of the operational effectiveness and suitability of CM/CCM systems.

Specifically, the Center:

- Determines performance and limitations of missile warning and aircraft survivability equipment (ASE) used on rotary-wing and fixed-wing aircraft
- Determines effectiveness of precision guided weapon (PGW) systems and subsystems when operating in an environment degraded by CMs
- Develops and evaluates CM/CCM techniques and devices
- Operates unique test equipment that supports testing across the DOD
- Provides analyses and recommendations on CM/CCM effectiveness to Service Program Offices, DOT&E, DASD(DT&E), and the Services
- Supports Service member exercises, training, and pre-deployment activities

In FY16 the Center completed 32 T&E activities. These activities included operational/developmental tests for rotary- and fixed-wing ASE, PGWs, threat data collection, experimentation tests, and pre-deployment/exercise support using CM/CCM. The Center conducted analysis of more than 30 DOD systems or subsystems – with special emphasis on rotary-wing survivability – and reported the results.

The Center provided T&E support throughout the year as follows:

- ASE testing, primarily in support of Joint Urgent Operational Needs Statement (JUONS) and Urgent Universal Needs Statement (UUNS) (approximately 40 percent)
- PGW, foreign system, and other types of field testing not related to ASE (approximately 22 percent)
- Realistic Man Portable Air Defense System (MANPADS) threat environment for Service member aircrew training (approximately 8 percent)
- Internal programs to improve test capabilities and develop test methodologies for new types of T&E activities (approximately 26 percent)
  - The Center continued to improve, develop, and validate multiple test tools for evaluating ASE infrared countermeasure (IRCM) systems.
  - In addition, the Center is improving its electronic warfare capability by developing and validating the Portable Range Threat Simulator (PRTS), which will provide a more comprehensive, integrated ASE T&E environment.
- Subject matter expertise to numerous working groups (WGs) and task forces (approximately 4 percent)

The Center's FY16 activities are summarized in the following subsections.

JUONS SUPPORT

Army: Advanced Threat Warning (ATW) Flare Interference Tower Test

- Sponsors: Technology Applications Program Officer (TAPO) and the 160th Special Operations Aviation Regiment (SOAR) Systems Integration Management Office (SIMO)
- Activity: The Center provided one Multi-Spectral Sea and Land Target Simulator (MSALTS) to perform two color, infrared (IR) missile simulations and jam beam data collection. The Center also provided missile warning sensor (MWS) subject matter expertise. This test focused on the ATW Directed Infrared Countermeasure (DIRCM) capabilities to maintain track of a MANPADS in the presence of flares.
- Benefit: The Center's participation in this test was in direct support of ongoing TAPO JUONS efforts. The data the Center collected during this test helped TAPO evaluate the ATW DIRCM's tracking capabilities in the presence of flares.

Army: Project Management Office Aircraft Survivability Equipment (PMO ASE) Formal JUONS Demonstration Pallet Test

- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS to perform simultaneous ultraviolet (UV) and IR missile simulations and jam beam data collection. The Center also provided MWS subject matter expertise. This test evaluated the ATW system. The ATW system was on a pallet installed on the UH-60M. UV simulations were used to assess Common Missile Warning System (CMWS) responses; IR simulations were used to assess ATW responses; and jam beam radiometers were used to assess ATW jam return.
- Benefit: The Center's participation in this test was in direct support of ongoing PMO ASE JUONS efforts. The data the

Center collected during this test helped PMO ASE assess the performance of the integrated ATW/CMWS.

Army: TAPO JUONS Demonstration Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided two MSALTS to perform two-color IR missile simulations. The Center also provided MWS subject matter expertise. This test evaluated the ATW system. The ATW system was on a pallet installed on the UH-60A. This test familiarized TAPO with IR MWS testing. The Center provided an independent assessment of ATW detection and angle-of-arrival (AOA) capabilities. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's involvement in the program was in direct support of ongoing TAPO JUONS efforts. The Center's independent assessment and the data it collected during this effort helped TAPO determine the ATW system's detection and threat AOA capabilities, which in turn will help them plan future JUONS test activities.

Army: PMO ASE JUONS Hostile Fire Indication Tower Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS – to perform simultaneous UV and IR missile simulations – and jam beam radiometers. This test assessed the capability of the ATW/CMWS-integrated system to track and place laser energy on the true target (MSALTS) with competing sources in the ATW DIRCM tracker field of view. The Center provided near real-time data reduction and analysis of simulations quality and jam onset times to assist the sponsor in test decisions.
- Benefit: The data the Center collected during this test helped PMO ASE assess the integrated ATW/CMWS's performance capabilities in the presence of competing sources.

Army: PMO ASE Formal JUONS IT3 Phase 2 Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS and one Joint Mobile Infrared Countermeasure Test System (JMITS) to perform simultaneous UV and IR missile simulations along with jam beam radiometers. The Center provided simulators for single and dual threat engagements against the integrated ATW/CMWS system as installed on the AH-64E.
- Benefit: The data the Center collected during this test helped PMO ASE assess the integrated ATW/CMWS system declaration, as well as threat AOA performance and DIRCM slew and pointing accuracy.

Army: PMO ASE Formal JUONS IT3 Clutter Flight Testing
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS – to perform simultaneous UV and IR missile simulations – and jam beam radiometers. The test evaluated the integrated ATW/CMWS system as installed on the AH-64E. The AH-64E flew in the Houston area with MSALTS placed in an urban/industrial environment. The objective was to determine the integrated ATW/CMWS's capabilities to detect and declare the MSALTS simulations in the presence of clutter.
- Benefit: The data the Center collected during this test helped PMO ASE assess the AH-64E integrated system's capability to declare, track, and respond when presented with simulated missiles in a clutter environment.

Army: Army Special Operation Aviation JUONS Phase 1a and 1b Flight Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided one JMITS to perform two-color IR missile simulations. The test evaluated the ATW, which was on the MH-60M upturned exhaust system (UES) for Phase 1a testing and on the MH-47F for Phase 1b testing. The test assessed the ATW system's declaration and threat AOA performance, as well as DIRCM slew and pointing accuracy.
- Benefit: The Center's participation in this test was in direct support of ongoing TAPO JUONS efforts. The data the Center collected during this test allowed TAPO to investigate the use of smart dispensing for IRCM flare sequences (i.e., dispense the best pattern based on threat AOA).

Air Force: Air Force Special Operations Command JUONS CV-22 ATW Sensor Flight Test
- Sponsor: 413th Flight Test Squadron Special Systems, Air Force Life Cycle Management Center
- Activity: The Center provided two MSALTS missile simulators to perform two-color IR simulations, as well as a laser van to conduct laser illuminations. The Center also provided test support to include consultation regarding test preparation, planning and execution, as well as data reduction, analysis and reporting for the missile simulations and laser illuminations. The test evaluated the Large Aircraft Infrared Countermeasure (LAIRCM) ATW system as integrated on the CV-22 platform.
- Benefit: The data the Center collected during this test helped the Air Force assess the performance of the ATW system as integrated on the CV-22 platform.

UUNS SUPPORT

Navy: Department of the Navy (DON) LAIRCM ATW MV-22 UUNS IT2A and B Flight Testing
- Sponsors: Program Executive Officer, Advanced Tactical Aircraft Protection Systems (PMA-272) and Commander, Operational Test and Evaluation Force (COTF)
- Activity: The Center provided two MSALTS to perform two-color IR missile simulations, threat-representative lasers, PRTS, and consultation regarding test preparation, planning and execution for the missile simulator and laser test events. This test was an end-to-end, open-air test and evaluation of the

UUNS for integration of the DON LAIRCM ATW system onto the MV-22. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's independent assessment and the data it collected during this effort helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the MV-22 and test the new ATW software upgrades.

Navy: DON LAIRCM ATW MV-22 Quick Reaction Assessment Flight Testing
- Sponsors: PMA-272 and COTF
- Activity: The Center provided two MSALTS (to perform two-color missile simulations), threat-representative lasers, and consultation regarding test preparation, planning and execution for the missile simulator and laser test events. This test was an operational test and evaluation of the UUNS for integration of the DON LAIRCM ATW system onto the MV-22.
- Benefit: The Center's participation in this test was in support of MV-22 ATW quick reaction operational testing. The data the Center collected during this test helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the MV-22.

ASE ACTIVITIES

Army: Seeker Performance in a Cluttered Environment Test
- Sponsors: Army Research Laboratory (ARL) and Utility Helicopters Project Office (UHPO)
- Activity: The Center provided the Seeker/Radiometric Test System (SRTS) with eight preemptive-configured IR surface-to-air missile (SAM) seekers, IR radiometric imagers, and SAM subject matter expertise during acquisition testing. This test evaluated the ability of MANPADS to acquire Army rotary wing aircraft flying against a cluttered terrain background. The radiometric and imagery data collected were used to quantify the background. After the test, the Center provided an independent assessment of the SAMs for incorporation into a briefing for ARL and UHPO.
- Benefit: The Center's involvement in this activity was in support of ARL's modeling and simulation efforts. The Center's independent assessment and the data it collected during this effort will help validate modeling and simulation of rotatory wing aircraft flying in a cluttered background environment against MANPADS.

Army: Reduced Optical Signature Emissions Solution IRCM IX Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided the SRTS with eight post-reactive-configured IR seekers and subject matter expertise during the IRCM effectiveness test for the MH-60M and MH-47G aircraft. These tests evaluated new flare CM sequences and variations of current flare CM sequences using improved flares, different flares, and/or flare timing within the sequences. The Center provided near real-time data reduction and analysis of flare sequences as well as on-site recommendations on flare sequence timing and/or pattern adjustments. As a result, the sponsor was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report and a briefing of test results to TAPO leadership.
- Benefit: The Center's involvement in this activity helped TAPO determine a final IRCM flare solution. The Center's independent assessment and the data it collected during this effort allowed TAPO to procure the new flares needed to enhance the protection of the MH-60M and MH-47G aircraft against MANPADS.

Army: Seeker Bowl XI IRCM Test
- Sponsor: Armament Research, Development and Engineering Center (ARDEC), Pyrotechnics Division, Countermeasure Flare Branch
- Activity: The Center provided the SRTS with eight post-reactive-configured IR seekers and subject matter expertise during the IRCM effectiveness test for the AH-64E ASPI, UH-60M UES, UH-60L UES, UH-60L HIRSS, and CH-47F IRSS aircraft. These tests evaluated the fielded flare IRCM sequences and variations of the sequence with timing and/or pattern adjustments. The Center provided near real-time data reduction and analysis of flare sequences as well as on-site recommendations on flare sequence timing and/or pattern adjustments. As a result, the sponsor was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's involvement in this activity helped ARDEC determine a final IRCM flare solution and prepare its post-test briefing for its higher headquarters. The Center's independent assessment and the data it collected during this effort allowed ARDEC to change the fielded flare sequence for all but the CH-47F IR Suppression System, thus providing better protection for those aircraft against MANPADS. ARDEC also briefed the test results to PMO ASE and platform program managers.

Air Force: U-28 ATW Sensor Flight Test
- Sponsor: 46th Test Wing Test Squadron, Defensive Systems and Mobility Directorate, Air Force Life Cycle Management Center
- Activity: The Center provided one JMITS missile plume simulator and personnel to perform two-color IR simulations in support of flight testing. The Center also provided test support to include consultation regarding test preparation, planning, and execution, as well as data reduction, analysis, and reporting for missile plume simulations. After the test, the Center provided an independent assessment analysis report.

- Benefit: The Center's independent assessment and the data it collected during this effort helped the Air Force assess the performance of the ATW system installed on the U-28 platform.

Navy: KC-130J DON LAIRCM Integration Test
- Sponsor: PMA-272
- Activity: The Center provided two MSALTS and subject matter expertise during the planning and execution of integration testing of the DON LAIRCM ATW onto the KC-130J.
- Benefit: The Center's participation in this test helped support integration of the ATW system onto the KC-130J and testing of new ATW software upgrades. The data the Center collected during this test helped the Navy assess the performance of the ATW system as installed on the KC-130J.

FOREIGN EVENTS

Foreign: Static Burn Test/NATO Trial KANERVA
- Sponsors: The Joint Countermeasures Test and Evaluation (JCMT&E) WG and the Naval Research Laboratory (NRL)
- Activity: The Center, along with the Arnold Engineering Development Complex and the NRL, collected radiometric signature data on static rocket motor burns at Niinisalo, Pohjankangas, Finland. Participation was under the provisions of existing NATO agreements and data analysis was coordinated within the provisions of the four-nation Multinational Test and Evaluation Program's Air Electronic Warfare Cooperative Test and Evaluation Project Arrangement. Data was collected on five types of threat rocket motors. Model updates resulting from this effort will be used to improve JMITS/MSALTS simulations.
- Benefit: The data the Center collected during this test supports refinements to MWS threat algorithms.

RESEARCH AND DEVELOPMENT ACTIVITY

USD(AT&L)/Air Force: Space-based Hypertemporal Imaging Research and Development
- Sponsors: USD(AT&L) Coalition Warfare Program and Air Force Research Laboratory, Advanced Missile Warning Technologies
- Activity: The Center deployed and operated the Towed Airborne Plume Simulator (TAPS) to Woomera, Australia. This risk reduction activity supported research and development associated with space-based sensor detection of IR sources through varying cloud layers.
- Benefit: The Center's TAPS provided the sponsors with the ability to present a controlled IR source (i.e., location and signature) within a space-based sensor's field-of-view at desired weather conditions. The Center provided self-assessment quick-look reports within 24 hours of each mission, summarizing the simulator's performance for each event.

PGW CM ACTIVITIES

Navy: JSOW C-1 OT-IIIB Land IRCM Live Fire Flight Test
- Sponsor: COTF
- Activity: The Center supported a live-fire test of the JSOW C-1 missile against a stationary target. The Center provided a CM environment consisting of camouflage nets and IR smoke to obscure and modify the signature of the stationary target while the JSOW C-1 attempted to acquire, track, and hit the target. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's independent assessment and the data it collected during this test helped COTF determine if the JSOW C-1 missile had retained its stationary land target mission capability in a CM environment given the recent addition of a moving maritime target mission capability.

Army: Joint Air-to-Ground Missile (JAGM) System
- Sponsor: Joint Attack Munition Systems Project Office
- Activity: The Center, in conjunction with the Edgewood Chemical and Biological Center, Smoke and Target Defeat Branch, provided various battlefield atmospheric obscurants for test and evaluation of the JAGM in tower and captive flight environments.
- Benefit: These tests were conducted to characterize the performance of the JAGM guidance section and collect scene data for the guidance section sensors in the presence of CMs for the verification of Integrated Flight Simulation results.

TRAINING SUPPORT FOR SERVICE MEMBER EXERCISES

Red Flag 16-1 (January 25 – February 12, 2016) Nellis AFB, Nevada

Red Flag 16-2 (February 29 – March 11, 2016) Nellis AFB, Nevada

Emerald Warrior (May 2 – 13, 2016) Hurlburt Field, Florida
Advanced Integration/Joint Forcible Entry (June 7 – 21, 2016) Nellis AFB, Nevada
Red Flag 16-3 (July 11 – 29, 2016) Nellis AFB, Nevada
Red Flag 16-4 (August 15 – 25, 2016) Nellis AFB, Nevada

- Sponsors: Various
- Activity: The Center provided personnel and equipment to simulate a threat environment, as well as subject matter expertise, to observe aircraft ASE systems and crew reactions to this environment. Specifically, the Center simulated MANPADS threat engagements for participating aircraft. Additionally, the Center provided MANPADS capabilities and limitations briefings to pilots and crews and conducted familiarization training at the end of the briefings.
- Benefits: The Center's participation in these exercises provided realism to the training threat environment and enhanced the Service member pilots' and crews' understanding and use of CM equipment, especially ASE. The data the Center collected and provided to the trainers helped the units develop/refine their tactics, techniques, and procedures to enhance survivability.

T&E TOOLS

The Center continues to develop tools for T&E of ASE. The Joint Standard Instrumentation Suite (JSIS) and the MSALTS Ultraviolet Emitter Enhancement (MUVEE) projects were funded by USD(AT&L), the Test Resource Management Center; and the Central T&E Investment Program.

JSIS

JSIS is a transportable, fully-integrated instrumentation suite that will be used to collect signature; Time, Space, Position Information; and related threat missile and hostile fire munitions metadata. The transportability of JSIS will allow it to be used both in the United States and abroad to reduce costs and expand the types of threat data available in the United States. The Navy (PMA-272), Army (PMO ASE), and Air Force (LAIRCM System Program Office) have endorsed JSIS, and it will be an integral part of each program office's ASE development. The Center deployed and operated JSIS during a risk reduction activity at Redstone Arsenal, Alabama, in February 2016. The Center exercised the system in an operationally realistic environment and verified the performance of key system capabilities. Some anomalies were identified that could not be detected in a laboratory environment. Post-event analysis discovered the root cause of these anomalies and the engineering changes needed to resolve them prior to acceptance testing. Early detection and resolution of any anomalies mitigates the risk of such anomalies arising when JSIS is used to collect data during actual acquisition program events.

The JSIS Initial Operational Capability is expected to be completed in FY17. As part of the JSIS project, the Center managed a contract to develop a Doppler Scoring Radar to support missile and hostile fire signature data collections and model developments. It is a 10.08 – 10.56 GHz tunable continuous wave and frequency modulated continuous wave radar, providing three degrees of freedom information (X, Y, Z) in time and range rate information on acquired and tracked targets. The Doppler Scoring Radar radar is capable of acquiring 128 targets and tracking 3 targets. The radar supported JSIS Risk Reduction tests. Its TrackVue software – which supports radar configurations, calibration, operational functionality, and data analysis – was updated to version 1.5.1. Sixteen high-power amplifiers within the radar and one spare were repaired to reduce noise floor fluctuations.

JSIS initial operational capabilities were driven by near-term needs for operational testing with the Navy's Advanced Threat Warner. While it represents a significant step forward in fielding data collection capabilities, significant gaps and shortfalls remain to include expanded missile attitude data collection and additional signature instrumentation to support emerging ASE programs with associated modeling and simulation needs. The Center has been actively formulating a technical approach, cost estimate, and acquisition strategy to produce JSIS Phase II with the intent of securing sponsorship beginning in FY17.

MUVEE

The MUVEE is an engineering improvement to MSALTS that incorporates the Army's T-MALUS emitter and software. The MUVEE will improve UV performance to enhance support of Army operational testing of Common Infrared Countermeasure (CIRCM) integrated with CMWS. Acceptance testing of the MUVEE was completed on May 20, 2016. The system was deployed to Redstone Test Center during the week of May 23 to collect signature data in support of system validation, as well as conduct some field regression testing. Corrective actions for deficient items and documentation updates were completed the first week of June 2016, followed by delivery of the system to the Center.

TEST VANS

- The Center procured a new van to replace a legacy, off-road test van which is no longer field-worthy. The van will be used for video and radiometric data collection at remote test sites.
- The Center is modifying one of its existing vans for use as the JSIS control van. This van will allow rapid and efficient deployment of JSIS to test sites.
- The Center is developing a new van to serve as the Center's Remote Launcher System control and instrumentation van. This van will be capable of controlling up to two launch trailers simultaneously.

THREAT SIGNATURE GENERATION

In support of Army's PMO ASE, the Center is generating up to 60,000 threat signatures for the CIRCM program. Initial planning meetings and coordination with the threat integration laboratories have occurred. The Center briefed its threat signature generation process to the program, Army Test & Evaluation Command, and Army Validation WG. The Center submitted the standard operating procedure to the PMO ASE for review and signature. The signatures will be used in labs and open-air testing for evaluating CIRCM performance.

PRTS AND HIGH-POWERED PRTS (HPRTS)

The Center is internally funding the procurement of two RF threat emitters: PRTS and HPRTS. This was prompted by the Center's FY13 electronic warfare internal study and the increasing demand for test tools that support multi-spectral, integrated ASE threat environments. The low-powered PRTS system completed validation data collection in FY16, and an HPRTS capability is scheduled for delivery in FY17. These systems are designed to replicate short-range acquisition and targeting radar systems. Both systems will be validated to support operational testing of the APR-39D(V)2 Radar Warning Receiver/Electronic Warfare Management System.

JCMT&E WG

DOT&E and DASD(DT&E) co-chartered the JCMT&E WG to measure, test, and assess the following:

- Aircraft self-protection, CMs, and supporting tactics
- Live-fire threat weapons and open-air T&E
- System performance in operationally relevant aircraft installations and combat environments
- T&E methodologies, instrumentation, analysis, and reporting
- Overseas threat and air electronic warfare systems performance and effectiveness data collection in coalition warfare environments

DOT&E, DASD(DT&E), all four of the U.S. Services, Australia, Canada, New Zealand, the UK, and the 22-nation NATO Air Force Armaments Group Sub-Group 2 participate in the JCMT&E WG. The WG is tasked with actively seeking mutually beneficial T&E opportunities to measure performance and suitability data, which are necessary to provide relevant operational information to deploying joint/coalition Service members and to U.S. acquisition decision makers. Specific efforts include:

- The JCMT&E WG has initiated discussions with European Command's Office of Defense Cooperation to conduct testing and data collection in its area of responsibility under operationally relevant environments important to the Combatant Command, Warfare Centers, and Programs of Record.
- The JCMT&E WG is cooperating with NATO partners and Partnership for Peace nations to provide opportunities to obtain and expand operationally relevant information in order to field new capabilities rapidly and reduce cost. The JCMT&E WG is building on the Center's proven record of conducting successful ASE data collection by coordinating live firings of radio frequency/electro-optical/IR SAMs, Hostile Fire Indication, and anti-tank guided missile firings by active duty air-defense units and test organizations in Finland, Sweden, the UK and Bulgaria. These efforts will provide measured operational performance of actual, modern, multifunction radars and integrated air defense systems that pose threats to U.S. and allied forces.
- The JCMT&E WG is the U.S. Steering Committee Chairman for bilateral and multinational Test and Evaluation Program Cooperative T&E Project Arrangements with Australia, Canada, and the UK. The JCMT&E WG is currently developing similar agreements with Germany, Finland, Denmark and Sweden. These efforts have already expanded the availability of air-electronic warfare system performance and suitability data to improve aircraft survivability. They have also identified opportunities to use other member nations' T&E capabilities to support U.S. program efforts.

The JCMT&E WG worked with the United States, Australia, Canada, and the UK to conduct modeling and simulation in Canada to support a combined MANPAD/radio frequency threat test of ASE installed in helicopters and fixed-wing aircraft at the Woomera Test Range, South Australia. That September 2016 threat test, trial DESERTRIDER 16, was designed to assess a preliminary open-air test methodology appropriate for testing integrated ASE. Combining the four nations' captive seekers, actual and simulated emitters for fixed- and rotary-wing aircraft equipped with flares and decoys provided each nation with valid, measured data not available singularly. Follow-on testing is being planned for laser warning/countermeasures systems in the UK, cold weather environment data collection in Canada, and ASE performance and tactics verification in the United States.

Index

Index

FY16 INDEX OF PROGRAMS

A

Abrams M1A2 System Enhancement Program (SEP) Main Battle Tank (MBT) 141
AC-130J Ghostrider 339
Aegis Ballistic Missile Defense (Aegis BMD) 415
Aegis Modernization Program 189
AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) Program 193
AH-64E Apache 143
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) 343
Air Force Distributed Common Ground System (AF DCGS) 345
Air Operations Center – Weapon System (AOC-WS) 347
Amphibious Assault Vehicle (AAV) Survivability Upgrade (AAV-SU) 197
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS) 199
AN/BLQ-10 Submarine Electronics Warfare Support System 201
AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) Sonar 203
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite 205
Army Integrated Air & Missile Defense (IAMD) 145
Army Network Modernization 133

B

B-2 Defensive Management System Modernization (DMS-M) 351
Ballistic Missile Defense System (BMDS) 407
Battle Control System – Fixed (BCS-F) 353

C

CH-53K – Heavy Lift Replacement Program 207
Chemical Demilitarization Program – Assembled Chemical Weapons Alternatives (CHEM DEMIL-ACWA) 147
Close-in Weapon System (CIWS) – SeaRAM Variant 211
Command Web 149
Common Aviation Command and Control System (CAC2S) 213
Consolidated Afloat Networks and Enterprise Services (CANES) 217
Cooperative Engagement Capability (CEC) 219
CV-22 Osprey 355
CVN 78 *Gerald R. Ford* Class Nuclear Aircraft Carrier 221
Cybersecurity 441

D

DDG 51 Flight III Destroyer/Air and Missile Defense Radar (AMDR)/Aegis Combat System 231
DDG 1000 *Zumwalt* Class Destroyer 227

Defense Agencies Initiative (DAI).. 29
Defense Enterprise Accounting and Management System (DEAMS) 357
Defense Readiness Reporting System – Strategic (DRRS-S)... 37
Defensive Medical Information Exchange (DMIX) 33
Department of Defense (DOD) Teleport... 41
Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM).. 235
Distributed Common Ground System – Army (DCGS-A) 151
Distributed Common Ground System – Navy (DCGS-N) 237
DOD Healthcare Management System Modernization (DHMSM)... 43

E

E-2D Advanced Hawkeye.. 239
E-3 Airborne Warning and Control System (AWACS) Block 40/45 361
Expeditionary Transfer Dock (T-ESD) and Expeditionary Sea Base (T-ESB)... 241

F

F-22A Advanced Tactical Fighter 365
F-35 Joint Strike Fighter 47
F/A-18E/F Super Hornet and EA-18G Growler 245
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T).. 369

G

Geosynchronous Space Situational Awareness Program (GSSAP)... 371
Global Broadcast Service (GBS) System 373
Global Command and Control System – Joint (GCCS-J) 109
Global Positioning System (GPS) Enterprise 377
Ground-based Midcourse Defense (GMD)... 421

H

HELLFIRE Romeo and Longbow 153

I

Infrared Search and Track (IRST).. 249
Integrated Defensive Electronic Countermeasures (IDECM) 251

J

Javelin Close Combat Missile System – Medium 155
Joint Information Environment (JIE)... 113
Joint Light Tactical Vehicle (JLTV) Family of Vehicles (FoV) 157
Joint Space Operations Center (JSpOC) Mission System (JMS) 383

Joint Standoff Weapon (JSOW)....253
Joint Tactical Networks (JTN) Joint Enterprise Network Manager (JENM)....159
Joint Test and Evaluation (JT&E)....465
Joint Warning and Reporting Network (JWARN)....117

K

KC-46A....387
Key Management Infrastructure (KMI) Increment 2....119

L

LHA 6 New Amphibious Assault Ship (formerly LHA(R))....255
Littoral Combat Ship (LCS)....259
Live Fire Test and Evaluation (LFT&E)....427
Logistics Modernization Program (LMP)....163

M

M109A7 Family of Vehicles (FoV) Paladin Integrated Management (PIM)....167
Major Automated Information System (MAIS) Best Practices....23
Massive Ordnance Penetrator (MOP)....391
MH-60S Multi-Mission Combat Support Helicopter....279
Mid-Tier Networking Vehicular Radio (MNVR)....169
Mine Resistant Ambush Protected (MRAP) Family of Vehicles (FoV) – Marine Corps....285
Miniature Air Launched Decoy (MALD) and Miniature Air Launched Decoy – Jammer (MALD-J)....393
MK 54 Lightweight Torpedo and Its Upgrades Including High Altitude Anti-Submarine Warfare Capability....287
Mobile User Objective System (MUOS)....291
MQ-4C Triton Unmanned Aircraft System....295
MQ-8 Fire Scout....297
MQ-9 Reaper Armed Unmanned Aircraft System (UAS)....395
MV-22 Osprey....301

N

Near Real Time Identity Operations (NRTIO)....173
Network Integration Evaluation (NIE)....137
Next Generation Diagnostic System (NGDS) Increment 1....123
Next Generation Jammer (NGJ) Increment 1....303

O

P

P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)....305

Patriot Advanced Capability-3 (PAC-3) 175
Problem Discovery Affecting OT&E 13
Program Oversight 7
Public Key Infrastructure (PKI) Increment 2 125

Q

QF-16 Full-Scale Aerial Target (FSAT) 399

R

Remote Minehunting System (RMS) 309
Rolling Airframe Missile (RAM) Block 2 313
RQ-4B Global Hawk High-Altitude Long-Endurance Unmanned Aerial System (UAS) 401

S

Sensors / Command and Control Architecture 411
Ship Self-Defense for LHA(6) 315
Ship Self-Defense for LSD 41/49 319
Ship-to-Shore Connector (SSC) 321
Small Diameter Bomb (SDB) II 403
Soldier Protection System (SPS) 179
Space-Based Infrared System Program, High Component (SBIRS HIGH) 405
Spider Increment 1A M7E1 Network Command Munition 183
SSN 774 *Virginia* Class Submarine 323
Standard Missile-6 (SM-6) 325
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 329
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT) 331

T

Tactical Tomahawk Missile and Weapon System 335
Terminal High-Altitude Area Defense (THAAD) 423
Test and Evaluation Resources 451
Theater Medical Information Program – Joint (TMIP-J) 129
The Center for Countermeasures (CCM) 471

U

V

VH-92A Presidential Helicopter Replacement Program 337

W

Warfighter Information Network – Tactical (WIN-T) 185

X

Y

Z

DOT&E Activity and Oversight

DOD Programs

Army Programs

Navy Programs

Air Force Programs

Ballistic Missile Defense Systems

Live Fire Test and Evaluation

Cybersecurity

Test and Evaluation Resources

Joint Test and Evaluation

Center for Countermeasures

Index

www.dote.osd.mil