EXHIBIT R-2, RDT&E Budget Item Justification	**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7	**R-1 ITEM NOMENCLATURE** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)

COST ($ in Millions)	FY2008	FY2009	FY2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Total PE Cost	32.494	33.639	24.226					
0734 Information Systems Security	24.569	24.820	22.026					
R0734 Communications Security (ONR)	2.121	2.137	0.000					
X3230 Communications Security (ONR)	0.000	0.000	2.200					
9999 Congressional Increases	5.804	6.682	0.000					
Quantity of RDT&E Articles								

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION:

(U) The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and Joint telecommunications and information systems from hostile exploitation and attack. ISSP is the Navy's implementation of statutory and regulatory requirements specified in Presidential Decision Directive 63, the Computer Security Act of 1987 (Public Law 100-235), Appendix III of Office of Management and Budget (OMB) Circular A-130, and Department of Defense Directive 8500.1. ISSP activities address the triad of Defensive Information Operations defined in Joint Publication 3-13; protection, detection, and reaction. Evolving detection and reaction responsibilities extend far beyond the traditional ISSP role in protection or Information Security (INFOSEC). Focused on FORCEnet supporting the highly mobile forward-deployed subscriber, the Navy's implementation of Network-Centric Warfare (NCW) places demands upon the ISSP as the number of users dramatically increases and the criticality of their use escalates. Today, the ISSP protects an expanding core service critical to the effective performance of the Navy's mission, supported by Mission Assurance Category 1 systems and Crypto Modernization requirements with Chairman Joint Chiefs of Staff Instruction (CJCSI) 6510.

(U) The interconnectivity of Naval networks, connections to the public information infrastructure, and their use in modern Naval and Joint war fighting means that FORCEnet is a more easily attainable and extremely high value target. An adversary has a much broader selection of attack types from which to choose than in the past. In addition to the traditional attacks that involve the theft or eavesdropping of information, United States Navy (USN) information and telecommunications systems face advanced attacks involving malicious changes to critical information, changes to the functioning of critical systems, denial of service (jamming), and the destruction of systems and networks. Since many Naval information systems are based on commercially available technologies, an adversary often has access to the very technologies they want to exploit.

(U) The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. ISSP provides the Navy's war fighter the essential information trust characteristics of availability, confidentiality, integrity, authentication, privacy, and non-repudiation. Information Assurance (IA) technology mix and deployment strategies must evolve quickly to meet the rapidly evolving threats and vulnerabilities.

EXHIBIT R-2, RDT&E Budget Item Justification	**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY / BA-7	**R-1 ITEM NOMENCLATURE** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)

(U) The Navy Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDTE) program works to provide the Navy with these essential Information Assurance (IA) elements: (1) Assured separation of information levels and user communities, including coalition partners; (2) Assurance of the telecommunications infrastructure; (3) Assurance of Joint user enclaves, using a defense-in-depth architecture; (4) Assurance of the computing base and information store; and, (5) Supporting assurance technologies, including a Public Key Infrastructure (PKI) and directories. Modeling Department of Defense (DoD) and commercial information and telecommunications systems evolution (rather than being one-time developments), the ISSP RDT&E program must be predictive, adaptive, and technology coupled. The program develops frameworks, architectures, and products based on mission threats, information criticality, exploitation risks, risk management, and integrated Joint information system efforts.

(U) All ISSP RDT&E efforts comply with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) as implemented through Office of Management and Budget (OMB) Circular A-119 of February 10, 1998, DoD Instruction 4120.24, Defense Standardization Program (DSP), and DoD Instruction 4120.3-M, Defense Standardization Program Policies and Procedures. The predominant commercial standards bodies in ISSP-related matters include International Organization for Standardization (ISO), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and National Institute of Standards and Technologies (NIST). The Joint interoperability required in today’s telecommunications systems makes standards compliance a must and, the ISSP RDT&E program complies with the Joint Technical Architecture. The FORCEnet architecture and standards documents reflect this emphasis on interoperable standards.

(U) The interconnection of FORCEnet into the DoD Global Information Grid (GIG) requires all ISSP RDT&E activities to adopt a minimum standard of “best commercial IA practice.” The ISSP RDT&E program examines commercial technologies to determine their fit within the USN architectures, provides feedback to vendors about what the Navy requires, and participates in the standards bodies themselves. When necessary to protect mission critical systems specified in Clinger/Cohen Act, the ISSP RDT&E develops or tailors commercial and government technologies, standards, and processes to meet Navy-unique requirements; prototypes systems or portions of systems and examines their utility in operational Navy settings; and, provides IA expertise and engineering to Navy and Joint information system developments. All ISSP technology development efforts solve specific Navy and Joint IA problems using techniques that speed transition to procurement as soon as ready.

(U) JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade and integration of existing, operational systems. This includes cryptographic systems required to protect information defined in 40 United States Code (USC) Chapter 25 Sec 1452, and the ISSP cryptographic RDT&E program is the implementation of requirements in Executive Orders 12333 and 12958 and National Security Decision Directive 145.

Major focus areas in FY10:

** Computer Network Defense (CND) – Develop User Defined Operational Picture (UDOP) to enhance Security Information Management (SIM) tools. Move to a Afloat Core Services(ACS) and Common Computing Environment (CCE).

** Crypto/Crypto Modernization – Continue to define prioritization of cryptographic products and strategies to modernize and reduce the overall crypto inventory. Continue development of Link-16 Common Cryptologic Module (CCM) and Link 22 Modernized Link Level Comsec (MLLC). Transition the Secure Voice research and development efforts to Crypto Modernization program for Special Test Equipment (STE) management and sustainment, and the fielding of the VINSON Advanced Narrowband Digital Voice Terminal (ANDVT) Cryptographic Modernization (VACM). Initiate the development of KW-46 Fleet Submarine Broadcast System (FSBS). Initiate the KL-51 major acquisition development. Investigate and if needed, develop a modernization plan for portable tactical radios and Demand Assigned Multiple Access (DAMA) crypto modernization requirements that is coordinated with National Security Agency (NSA) and across the Services.

** Electronic Key Management Sysytem(EKMS)/ Tactical Key Loader (TKL)/ - Complete development, first article testing and transition to production.
** EKMS/ Key Management Infrastructure(KMI) - Transition planning; participation in KMI Operational Assessment #2 (OA2) and Initial Operational Test and Evaluation to support upcoming milestone C

EXHIBIT R-2, RDT&E Budget Item Justification	**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RESEARCH DEVELOPMENT TEST & EVALUATION, NAVY/BA-7	**R-1 ITEM NOMENCLATURE** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)

(U) B. PROGRAM CHANGE SUMMARY:

(U) Funding:	FY 08	FY 09	FY10
FY 09 President's Budget	34.337	27.037	24.404
FY 10 President's Budget	32.494	33.639	24.258
Total Adjustments	-1.843	6.602	-0.146

Summary of Adjustments			
Congressional Rescissions			
Congressional Adjustments	0.000	6.700	0.000
Program Adjustments	-1.843	0.000	0.000
Rate/Misc Adjustments		-0.098	-0.146
Subtotal	-1.843	6.602	-0.146

(U) Schedule:

- The KG40-AR Decision/Award has slipped from 1Q FY08 to 2Q FY08 due to environmental qualification testing. Production contract has been awarded.
- Electronic Key Management System (EKMS) Phase V software Local Comsec Management Software (LCMS) 5.1 delivery has slipped from 2Q FY08 to 4Q FY09 due to National Security Agency (NSA) testing delays.
- LMCS 5.2 software delivery is now reflected in 2Q FY10.
- KG45-A deliveries have slipped from 2Q FY08 to 3Q FY09 due to NSA certification qualification testing requirements

(U) Technical:

N/A.

Exhibit R-2, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Project Justification								**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY	**PROGRAM ELEMENT NAME AND NUMBER**			**PROJECT NUMBER AND NAME**				
RDT&E, N / BA-7	0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)			0734 INFORMATION SYSTEMS SECURITY				
COST ($ in Millions)	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Project Cost	24.569	24.820	22.026					
RDT&E Articles Qty								

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION: The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDTE) provides Information Assurance (IA) solutions for the Unites States Navy (USN) forward deployed, highly mobile information subscriber. FORCEnet relies upon an assured information infrastructure, and the ISSP RDT&E program architects, engineers, and provides the Quality of Assurance (QA) consistent with risks faced. The ISSP addresses engineering design, development, modeling, test, and evaluation for the unique IA challenges associated with the highly mobile, dispersed, bandwidth limited, and forward-tactical connected USN communications systems.

(U) ISSP RDT&E must work closely within the Navy's Information Operations – Exploit (Signals Intelligence - SIGINT) and Information Operations – Attack (INFOWAR - information warfare) communities. ISSP RDT&E developed systems must dynamically change the Navy's current information assurance posture, based upon operational indications and warnings. To ensure interoperability, ISSP RDT&E must integrate fully with the FORCEnet and Maritime Cryptologic Architectures. ISSP RDT&E developed systems can provide the trigger for offensive warfare activities, such as those developed by the Navy Information Operations Command (NIOC).

(U) This program element includes a rapidly evolving design and application engineering effort to modernize National Security-grade (Type-1) cryptographic equipment and ancillaries with state-of-the-art replacements in order to counter evolving and increasingly sophisticated threats. Communication Security (COMSEC) and Transmission Security (TRANSEC) evolution is from stand-alone dedicated devices to embedded modules incorporating National Security Agency (NSA) approved cryptographic engines, loaded with the certified algorithms and key, and interconnected via industry-defined interfaces. This includes the Department of Defense (DoD) Global Information Grid (GIG) Capabilities Requirements Document (CRD) for the development of Content Based Encryption (CBE) continuing in Fiscal Year (FY) 2006-2011.

(U) In addition to protecting National Security information, ISSP RDT&E must provide enterprise-wide assurance for statutorily protected information under the Privacy Act of 1974, Computer Matching and Privacy Protection Act of 1988, Medical Records Confidentiality Act of 1995, Model State Public Health Privacy Act, 45 Code of Federal Regulation (CFR) subtitle A sub-chapter C, parts 160- 164, 1999, and the Federal Education Records Privacy Act. ISSP RDT&E efforts must also provide assurance to the broad spectrum of Sensitive-but-Unclassified (SBU) information such as financial, personnel, contractor proprietary, and procurement sensitive.

(U) The ISSP today includes much more than legacy Communications Security (COMSEC) and Network Security (NETSEC) technology. IA or Defensive Information Operations, exists to counter a wide variety of threats in a Navy environment. ISSP activities cover all telecommunications systems, and RDT&E projects must provide protection, detection, and reaction capabilities to the operational commander. ISSP RDT&E provides dynamic risk managed IA solutions to the Navy Information Infrastructure, not just security devices placed within a network.

(U) Few technology areas change as fast as telecommunications and computers, and IA must keep pace. This results in the continuing need to evaluate, develop, and/or test IA products and approaches. Technology-based efforts include developing or applying: (1) new secure voice prototypes; (2) technology for a new family of programmable COMSEC and Transmission Security TRANSEC modules; (3) security appliances and software for switched and routed networks; (4) technology to interconnect networks of dissimilar classification, known as Cross Domain Solutions (CDS); (5) techniques for assuring code and data residing in and transiting the Navy's computing base and information store; and (6) Public Key Infrastructure (PKI) and associated access control technologies (such as SmartCards and similar security tokens).

(U) The resulting expertise applies to a wide variety of Navy development programs that must integrate IA technology. Unlike traditional single-product development programs, the ISSP RDT&E holds a unique Navy-enterprise responsibility outlined in SECNAVINST 5239.3 and OPNAVINST 5239.1C.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

(U) The Information Systems Security Program (ISSP) Research Development Test & Evaluation (RDTE) efforts must conclude with certified and accredited systems. This requires (1) assured separation of information levels and user communities, including coalition partners; (2) assurance of the telecommunications infrastructure; (3) assurance of Joint user enclaves; (4) assurance of the computing base and information store; and, (5) supporting assurance technologies, including Public Key Infrastructure (PKI) and directories. To ensure interoperability and commercial standards compliance, these efforts often encompass the research, selective evaluation, integration, and test of commercial-off-the-shelf/Non-Developmental Item (NDI) Information Assurance (IA) security products. For example, evaluation may include defensible network boundary capabilities such as firewalls, secure routers and switches, guards, Virtual Private Networks (VPN), and network Intrusion Prevention Systems (IPS).

(U) The current operating environment has virtually eliminated the traditional distinction between telecommunications and information systems. Because (IA) is a cradle-to-grave enterprise-wide discipline, this program applies the technology and methodology to systems in development, production and operation, and develops the infrastructure needed to support and evaluate the security of deployed systems. The following describes several major ISSP technology areas:

(U) Under the Navy Secure Voice (NSV) program, ISSP RDT&E assesses technology to provide high grade, secure tactical and strategic voice connectivity.

(U) Under the Navy Cryptographic Modernization Program, ISSP RDT&E provides high assurance and other cryptographic technologies protecting information and telecommunication systems.

(U) Under the Navy Security Management Infrastructure (SMI) program, ISSP RDT&E develops, evaluates, and applies new emerging technology and enhanced capabilities to the Electronic Key Management System (EKMS)/KMI and other Navy Information Systems. Additional efforts will focus on the architecture, design, and development of systems to manage the security parameters (i.e., cryptographic keys) necessary to the operation of the systems developed by the Secure Data and Secure Voice portions of the ISSP. This includes the application of PKI and Certificate Management Infrastructure (CMI) technology, and the development of improved techniques for key and certificate management to support emerging, embedded cryptographic technology.

(U) Under the Secure Data program, efforts focus on architectures, designing, acquiring, demonstrating and integrating the IA technologies into FORCEnet and the Navy Marine Corp Intranet (NMCI). This portion of the ISSP supports delivery of network security engineering expertise needed to support the NMCI, outside the continental United States (OCONUS) Navy Enterprise Network (ONE-NET), and the Integrated Shipboard Network Systems (ISNS), along with constituent systems such as Automated Digital Network System (ADNS), Global Command and Control System - Maritime (GCCS-M). Begin transitioning to an Open Architecture (OA) in support of the Consolidated Afloat Networks and Enterprise Services (CANES) Common Computing Environment (CCE) and Afloat Core Services (ACS). It includes activities to:

- Ensure that the United States Navy (USN) telecommunications and networks follow a consistent architecture and are protected against denial of service.
- Ensure that all data within the USN Enterprise is protected in accordance with its classification and mission criticality, as required by law.
- Provide the ability to protect from, react to, and restore operations after an intrusion or other catastrophic event.
- Support the USN Computer Network Defense (CND) Service Provider Enabler by providing IA response to Information Operation Conditions (INFOCONs).
- Defend against the unauthorized modification or disclosure of data sent outside enclave boundaries.
- Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.
- Provide strong authentication of users sending or receiving information from outside their enclave.
- Defend against the unauthorized use of a host or application, particularly operating systems.
- Maintain configuration management of all hosts to track all patches and system configuration changes.
- Ensure adequate defenses against subversive acts of trusted people and systems, both internal and external.
- Transition to CCE.
- Transition to ACS.

Exhibit R-2a, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

- Provide a cryptographic infrastructure that supports key, privilege and certificate management; and that enables positive identification of individuals utilizing network services.
- Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that enables rapid detection and reaction to intrusions and other anomalous events, and that enables operational situation awareness.

(U) JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade of existing, operational systems.

Exhibit R-2a, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

(U) B. Accomplishments/Planned Program

	FY 08	FY 09	FY 10	FY 11
Computer Network Defense (CND)	8.806	8.681	8.055	
RDT&E Articles Quantity				

FY 08: Completed the security situational awareness technologies for knowledge empowered Computer Network Defense (CND) operations for both ship and shore installations. Established system management capabilities to enforce proactive unit level security policies across the Navy Network Enterprise to centrally manage security policies to controllable devices such as Firewalls, Intrusion Prevention Systems (IPS), and Filtering Routers at shore based Network Operations Centers (NOC). Included Information Assurance (IA) appliances, software, and implementation techniques for automated response products such as vulnerability remediation, Information Operation Condition (INFOCON) response, and intrusion prevention policies. Completed the development and integration of the patch management and host based security agents tools. Developed additional tools to determine accurate asset location and inventory information. Initiated the development of the process to assign asset criticality at the host and application level through the use of the data in the new tool. Integrated Joint Task Force-Global Network Operations (JTF-GNO) IA applications and implemented Component Task Orders (CTO) for Joint policies such as Information Assurance Vulnerability Alert (IAVA) scanning and remediation, Information Operation Condition (INFOCON) response, and Host Based Security Solution (HBSS) policy. Translated IA engineering and FORCEnet capabilities into an initial program Capability Production Document (CPD) to acquire advanced CND solutions to support a range of initiatives meeting Joint Command-Control IA & security situational awareness, Navy tactical edge attack sensing & warning, and cyber defense indications & warning in information sharing network operations. Conducted a pilot to address data-at-rest protection on mobile and removable devices.

FY 09: Continue system integration efforts with analytical tools to identify asset criticality at the host and application level. Develop computer-network evaluation capabilities to perform real-time metrics of operational compliance with IA security controls, Mission Assurance Category, and Data Confidentiality. Evolve system incremental capabilities to advance CND Protect, Monitor, Detect, Analyze, and Respond. Conduct Honey Net Research to develop proactive Insider Threat Countermeasures and Application Layer Content Scanning. Develop User Defined Operational Pictures (UDOP) to enhance Security Information Manager (SIM) tools with active defense capabilities, improved incident correlation, and situation awareness reporting. Complete the development of the process to assign asset criticality at the host and application level. Initiate the development of new capabilities to support the selective and automatic reactive settings of the network in accordance with INFOCON policies. Address the capabilities required to support the INFOCON management at both the Naval Cyber Defense Operation Center (NCDOC) and the Fleet NOC level.

FY10: Begin the development of the process to assign asset criticality at the host and application level. Advance development of proactive Insider Threat Countermeasures and application layer security risk monitoring. Develop User Defined Operational Pictures (UDOP) to enhance Security Information Management (SIM) tools. Initiate research to analyze Information Assurance capabilities to support Afloat Core Services (ACS) systems with selective and autonomic settings on the CND posture as a proactive response to threat attack sensors and vulnerability indications. Address the capabilities required to support CND management of a ACS platform from a tiered enclave organizational level, network operations intermediate level, and global enterprise management level. Begin transition to Consolidated Afloat Network Enterprise Services (CANES) Increment 1.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Crypto/Crypto Modernization	6.638	8.729	7.339	
RDT&E Articles Quantity				

FY08: Completed development support efforts in coordination with the Information Systems Security Office, Joint Services, and the National Security Agency (NSA). Completed development efforts and acquisition documentation for identified and selected KEESEE Cryptographic products as the Integrated Product Team (IPT) completed at 100%. Completed SAVILLE Integrated Product Team (IPT) (90% Crypto's identified). Completed major preacquisition and development of specification for KGR-68. Provided consistent Information Assurance (IA) engineering support for on-going development of Crypto Modernization devices including Universal Crypto Device (UCD), KG-45, KL-51 and KG-68B. Completed development and testing of Cryptographic Module (Engine) in a joint effort with other services and a next generation cryptographic device for replacing identified legacy devices providing for secure communication capabilities to the war fighter. Completed additional pre-acquisition and development of on-going Decertified Cryptographic Algorithms affecting legacy Department of the Navy (DoN) Cryptographic Devices.

FY09: Continue to provide Cryptographic Products, including Type-1 United States (US) only, allied and coalition, and Commercial-Off-the-Shelf (COTS) to DoN. Continue research, evaluation, and prioritization of cryptographic products. Provide consistent IA engineering support for the development and integration of Crypto Modernization products and being major pre-acquisition and development specification for KGV-68. Complete development and testing of first UCD module in a joint effort with other services Begin installation of identified first device groupings. Continue development and testing of on-going Decertified Cryptographic Algorithms affecting legacy DoN Cryptographic Devices and Communication Security (COMSEC). Continue pre-acquisition and development of on-going Decertified Cryptographic Algorithms affecting legacy DoN Cryptographic Devices. Develop program documentaiton and way ahead Crypto identified devices. Continue to support the on-going Cryptographic Joint IPT. Continue pre-acquistion and development of LINK 16 Common Crypto Module (CCM), VINSON/ANDVT Crypto Mod (VACM), Programmable Objective Encryption Technologies (POET), KW-46 Fleet Submarine Broadcast System (FSBS), and Telemetry. The Crypto Modernization Program Office (CMPO) will be developing LINK 16, KW-46 and VACM. Modernizing these devices will provide replacments in accordance with the Joint Chief of Staff's modernization schedule and National Security Agency (NSA) planned decertification.

FY10: Continue research, evaluation, and prioritization of cryptographic products such as Demand Assigned Multiple Access (DAMA), portable tactical radios, Single Channel Ground and Airborne Radio System (SINCGARS), Integrated Broadcast Service Multi Mission Advanced Tactical Terminal (IBS MATT), and various embedded devices. Continue coordination with the Information Systems Security Office, Joint Services, and the NSA, including representing the Navy at the Joint Service Crypto Mod Working Group (JSCMWG). Continue identifying strategies to reduce the overall crypto inventory within the DoN to realize long term cost savings. Continue providing consistent IA engineering support for the development and integration of Crypto Modernization products. Continue to support to the on-going Cryptographic Joint Algorithm IPT. Continue development for the Link-16 CCM. Secure Voice research and development efforts will transition under CMPO, including Small Business Inovative Research (SBIR) oversight, and Naval Research Laboratory's (NRL) research into Secure Voice emerging technologies and related technical products. In addition, research and development funding support to the VACM program will transition to CMPO as well. The United States Navy (USN) will participate in the United States Air Force (USAF) led VACM program by providing Secure Voice technical support, documentation review, acquisition and logistic support, and test and evaluation support. Initiate major acquisition and development of KL-51. Continue acquisition efforts for development of KL-51M, KW-46M, Fixed Submarine Broadcast System (FSBS), and Link 22 Modernized Link Level Comsec (MLLC). Continue Crypto voice standardization based on the Variable Data Rate (VDR), Voice Compression Algorithm (VCA).

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Secure Voice	1.056	1.115	0.000	
RDT&E Articles Quantity				

FY08: Completed development and integration test of Submarine Secure Communication Interoperability Protocol (SCIP) Inter-Working Function (IWF) gateway to provide off-ship secure communication capabilities while underway. Completed development and tested a SCIP IWF to provide off-ship secure voice communications to underway Military Sealift Command (MSC) ships and Coast Guard ships. Completed development of the Variable Data Rate Voice Encoder and its baseline interface software. Completed generation of baseline functionality (derived from operational and mission requirements and new technologies) and design of a functional model for development of next generation secure voice products.

FY09: Complete development and integration test of the SCIP IWF for MSC and Coast Guard ships. Continue the design and development of next generation voice and Secure Voice capabilities for shipboard voice services modernization and consolidation. Continue Small Business Innovative Research (SBIR) phase II R&D efforts.

FY10: Transition from Secure Voice to the Crypto Modernization Program for VINSON/ANDVT Crypto Mod (VACM) and R&D technology efforts.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Key Management Infrastructure (KMI/EKMS/PKI)	5.228	4.043	0.000	
RDT&E Articles Quantity				

FY08: Completed streamline method for developing effective secure symmetric and asymmetric cryptographic key and generation, distribution, management, and usage products and services by identifying and prioritizing fleet requirements. Completed Electronic Key Management System (EKMS) Phase V to include development and implementation of an extended, networked architecture (key distribution over Secret Internet Protocol Router Network (SIPRNet) to improve distribution and reliability for deployed forces, modernized key processors, common user application software and data transfer devices. Completed Wireless Key Fill technology design and development. Completed review/ input for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) client and Advanced Key Processor (AKP) Capability Development Document (CDD), including testing and Hub Management Interface (HMI) development. Completed review of initial KMI CI-3 capability CDD development and design including Benign Fill and single point keying. Supported and ensured coordinated developments for KMI/EKMS in the transition from Internet Protocol Version 4 (IPV4) to IPV6. Completed security and functionality testing and evaluation of Public Key Infrastructure (PKI) tokens, readers and middleware for the SIPRNET. Researched security and functionality testing and evaluation of PKI Non-classified Information Protocol Router Network (NIPRnet) tokens and readers to upgrades to middleware, in support of the Homeland Security Presidential Directive 12 (HSPD-12) biometrics based smart cards. Completed research and development of solutions to resolve technical challenges and the tools required for deployment of both Navy non-Navy Marine Corps Internet (NMCI) Cryptographic Logon (CLO), CLO for non-Windows operating systems, and Navy Certificate Validation Infrastructure/On Line Certificate Status Protocol (NCVI/OCSP) Afloat. Researched and developed tools to support Microsoft VISTA implementation, PKI with IPv6 Device (non-human) Certificates, and signature applications/XML document signing. Completed development and integration of NCVI/OCSP ashore. Completed Defense Message System (DMS) migration to PKI. Supported the development and testing of Tactical PKI (as part of DoD KMI) and its supporting architecture.

FY09: Continue KMI CI-2 client and Advanced Key Processor (AKP) security testing and certification and accreditation. Continue Navy input to KMI CI-3 CDD development (led by National Security Agency NSA) for Advanced Extremely High Frequency (AEHF), Transformational Satellite (TSAT), and Global Information Grid (GIG) requirements for Navy. Research and integrate PKI device certificates for mobile devices using 802.1x interfaces. Continue security and functionality testing and evaluation of PKI Non-classified Information Protocol Router Network (NIPRnet) and Secret Information Protocol Router(SIPRnet) tokens and readers to support Tactical PKI and HSPD-12 implementation. Continue to research and develop solutions and tools for signature applications/XML document signing and Public Key Enabled (PKE).

FY10: Transition KMI efforts to define EKMS, PKI, and KMI technology areas.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Key Management Infrastructure (KMI)			2.522	
RDT&E Articles Quantity				

FY08: Transitioned from Key Management Infrastructure (KMI) to define Electronic Key Management System (EKMS), Public Key Infrastructure (PKI), and KMI technology areas.

FY09: Transition from KMI to define EKMS, PKI, and KMI technology areas.

FY10: Begin to finalize the Department of the Navy (DoN) KMI architecture and roll out strategy for deployment. Install KMI Manager Client/Advanced Key Processor (MGC/AKPs) at selected pilot sites in support of operational assessment. Identify any issues pertaining to transition from EKMS. Provide supporting information to Navy Acquisition Decision Memorandum (ADM**)** for full rate fielding within the Navy. Finalize Navy KMI Capability Increment 3 (CI-3) Capability Development Document (CDD) requirements. Continue engineering efforts for Navy transition and test planning for KMI CI-2 client and Advanced Key Processor (KP). Develop Navy implementation plan for KMI. Complete development of Tactical Key Loader (TKL), complete First Article and National Security Agency (NSA) Certification testing. Transition to production.

EXHIBIT R-2a, RDT&E Project Justification		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Public Key Infrastructure (PKI)			0.792	
RDT&E Articles Quantity				

FY08: Transitioned from Key Management Infrastructure (KMI) to define Electronic Key Management System (EKMS), Public Key Infrastructure (PKI), and KMI technology areas.

FY09: Transition from KMI to define EKMS, PKI, and KMI technology areas.

FY10: Initiate security and functionality testing and evaluation of multi-domain tokens, readers and middleware for the Non-Classified Internet Protocol Router (NIPR),Secret Internet Protocol Router (SIPR**),** and Tactical Public Key Infrastructure (PKI). Continue research and development of solutions to resolve technical challenges and the tools required for continued deployment of Navy non-Navy, Marine Corps Internet (NMCI) Cryptographic Log On (CLO) and Navy Certificate Validation Infrastructure/Online Certificate Status Protocol (NCVI**/**OCSP) Afloat. Research and develop tools to support Device (non-human) Certificates. Continue security and functionality testing and evaluation of PKI tokens and readers to support Tactical PKI and Homeland Security Presidential Directive-12 (HSPD-12) implementation. Support systems engineering during the integration process and the analysis/evaluation of new application updates including new Operating Systems (OSs (Windows and non-Windows) into Navy PKI environments. Provide for evaluation of Commercial -Off-the-Shelf (COTS) products that can support coalition information sharing. Initiate test and evaluation of HSPD-12 token and middleware as part of the transition to stronger algorithms. Research and develop tools to support PKI withInternet Protocol Version 6 (IPv6) and Suite B implementation.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Electronic Key Management System (EKMS)			0.427	
RDT&E Articles Quantity				

FY08: Transitioned from Key Management Infrastructure (KMI) to define Electronic Key Management System (EKMS), Public Key Infrastructure (PKI), and KMI technology areas.

FY09: Transitioned from KMI to define EKMS, PKI, and KMI technology areas.

FY10: Continue to define EKMS technology gaps in preparation to the transition to KMI . Identify technical solutions for EKMS sustainment until KMI CI-3.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NAME AND NUMBER** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

	FY 08	FY 09	FY 10	FY 11
Information Assurance Architectures	2.841	2.252	2.891	
RDT&E Articles Quantity				

****Transitioned from Emerging Technology**

FY08: Provided security systems engineering support for the development of the Department of Defense (DoD) and the Department of the Navy (DoN) Information Assurance (IA) architectures and the transition of new technologies to address Navy IA challenges. Supported the ongoing security design and integration of Computer Network Defense in Depth (CNDiD) products and services for the Navy's implementation of the Global Information Grid (GIG) via FORCEnet and major initiatives such as Transformational Communication (TC), Global Information Grid Enterprise Services (GIG-ES). Provided risk analysis and recommended risk mitigation strategies for Navy critical networks and Command, Control, Computers, Communications C4I systems. Coordinated with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provided IA engineering for development of Wireless Networks and Personal Digital Assistant (PDA) security readiness of Naval wireless networks and mobile computing devices.

FY09: Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Support the ongoing security design and integration of IA Components into initiatives such as FORCEnet via a coordinated and CNDiD strategy. Provide risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provide IA engineering for development of Wireless Networks and PDA security readiness of Naval wireless networks and mobile computing devices. Continue to evaluate products for security issues and develop guidance and procedures.

FY10: Continue to provide security systems engineering support for the development of DoD and DoN IA architectures and the transition of new technologies to address Navy IA challenges. Support the ongoing development of the Navy IA Master Plan and coordinate IA activities across the virtual System Command (SYSCOM) via the IA Technical Authority (TA) to ensure the security design and integration of CNDiD products and services is consistent across the Navy for major initiatives such as the future afloat, ashore, and Outside the Continental United States (OCONUS) networks. Provide IA risk analysis and recommended risk mitigation strategies for Navy critical networks and C4I systems. Coordinate with the Navy acquisition community to ensure IA requirements are identified and addressed within the development cycles for emerging Navy network and C4I capabilities. Provide IA engineering for development of Wireless Networks and PDA security readiness of Naval wireless networks and mobile computing devices. Continue to evaluate products for security issues and develop guidance and procedures for the design and integration of risk mitigation strategies via appropriate IA controls.

Exhibit R-2a, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Budget Item Justification		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NAME AND NUMBER 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
OPN 3415 Info Sys Security Program (ISSP)	**121.319**	**100.855**	**119.054**					

(U) D. ACQUISITION STRATEGY:

EKMS Phase V - The Navy's Information Systems Security Program (ISSP) Electronic Key Management System (EKMS) program is linked to the National Security Agency's (NSA) strategy in implementing EKMS in evolutionary phases and migrating to Key Management Infrastructure (KMI). NSA is the lead for the joint EKMS effort and has been developing and certifying EKMS devices and capabilities in an evolutionary approach. EKMS Phase V is a major component evolving to KMI Capability Increment 2 (CI-2). KMI is a Major Automated Information System (MAIS) program assigned to NSA. Therefore, it is crucial that the Research and Development efforts of EKMS coincide with those of KMI. Navy's EKMS requires Research, Development, Test and Evaluation (RDT&E) funding over the Future Years Defense Program (FYDP) to ensure the Navy infrastructure evolves with the EKMS phases, supports additional devices certified by NSA and supports the migration of EKMS to KMI CI-2. This will require potential modifications to the Navy EKMS architecture including the Local Management Device (LMD) and associated software. These efforts require close work with NSA and the other services to ensure no impact on current operations and minimum impact on EKMS Phase 5 as it evolves to KMI CI-2. NSA certified Commerical-Off-The-Shelf/Government-Off-The-Shelf (COTS/GOTS) devices are procured to support Navy requirements. The EKMS Phase V program will utilize existing competitively awarded NSA and Space and Naval Warfare Systems Centers (SSCs) contracts for development and implementation of type 1 certified COTS/GOTS devices for initial production phases, with plans to initiate innovative contracting methods and types consistent with current Assistant Secretary of the Navy Research, Development & Acquisition (ASN/RDA) policies to reduce cost and streamline the integration, installation, logistics and training efforts.

KMI - KMI is the next generation EKMS system that is net centric in nature, providing the infrastructure for management, ordering and distribution of key material as well as directly supporting the key requirements of all Crypto modernization efforts. Navy will continue to provide and refine Navy unique requirements into the NSA KMI CI-2 and CI-3 Capability Development Documents (**CDD**). In parallel, continue to define Navy operational architecture and requirements for roll out of this new capability in the Fiscal Year 2010/2011 timeframe.

Crypto Modernization (KW-46 Replacement) - Evaluating acquisition development replacements of the KG-45, KL-51, KG-68B cryptographic devices per the UCD effort, the Navy has refined the requirement specifications, preparing formal Analysis of Alternatives (AoA), Request For Information (RFIs), and Life Cycle Cost Estimates (LCCEs) in first quarter (1Q) Fiscal Year 2008.

Exhibit R-3 Cost Analysis (page 1)

DATE:
May 2009

APPROPRIATION/BUDGET ACTIVITY
RDT&E, N / BA-7

PROGRAM ELEMENT
0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)

PROJECT NUMBER AND NAME
0734 INFORMATION SYSTEMS SECURITY

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 09 Cost	FY 09 Award Date	FY 10 Cost	FY 10 Award Date	FY 11 Cost	FY 11 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Primary Hardware Development	C/CPFF	VIASAT, Carlsbad, CA	7.282							7.282	7.282	7.282
Primary Hardware Development	C/MIPR	MITRE, San Diego, CA	5.522							5.522	5.522	5.522
Primary Hardware Development	C/VAR	Various	85.489	3.118	VAR	5.483	VAR			Continuing	Continuing	Continuing
Systems Engineering	C/VAR	Various	86.246	11.310	VAR	10.080	VAR			Continuing	Continuing	Continuing
Subtotal Product Development			184.539	14.428		15.563				Continuing	Continuing	Continuing
Remarks:												
Software Development	CPAF	SAIC, San Diego, CA	32.877							32.877	32.877	32.877
Software Development	C/WX	NRL, Washington, D.C.	2.953	0.197	11/09	0.494	11/10			Continuing	Continuing	Continuing
Software Development	C/VAR	Various	2.408	1.217	11/09	1.088	11/10			Continuing	Continuing	Continuing
Subtotal Support			38.238	1.414		1.582				Continuing	Continuing	Continuing

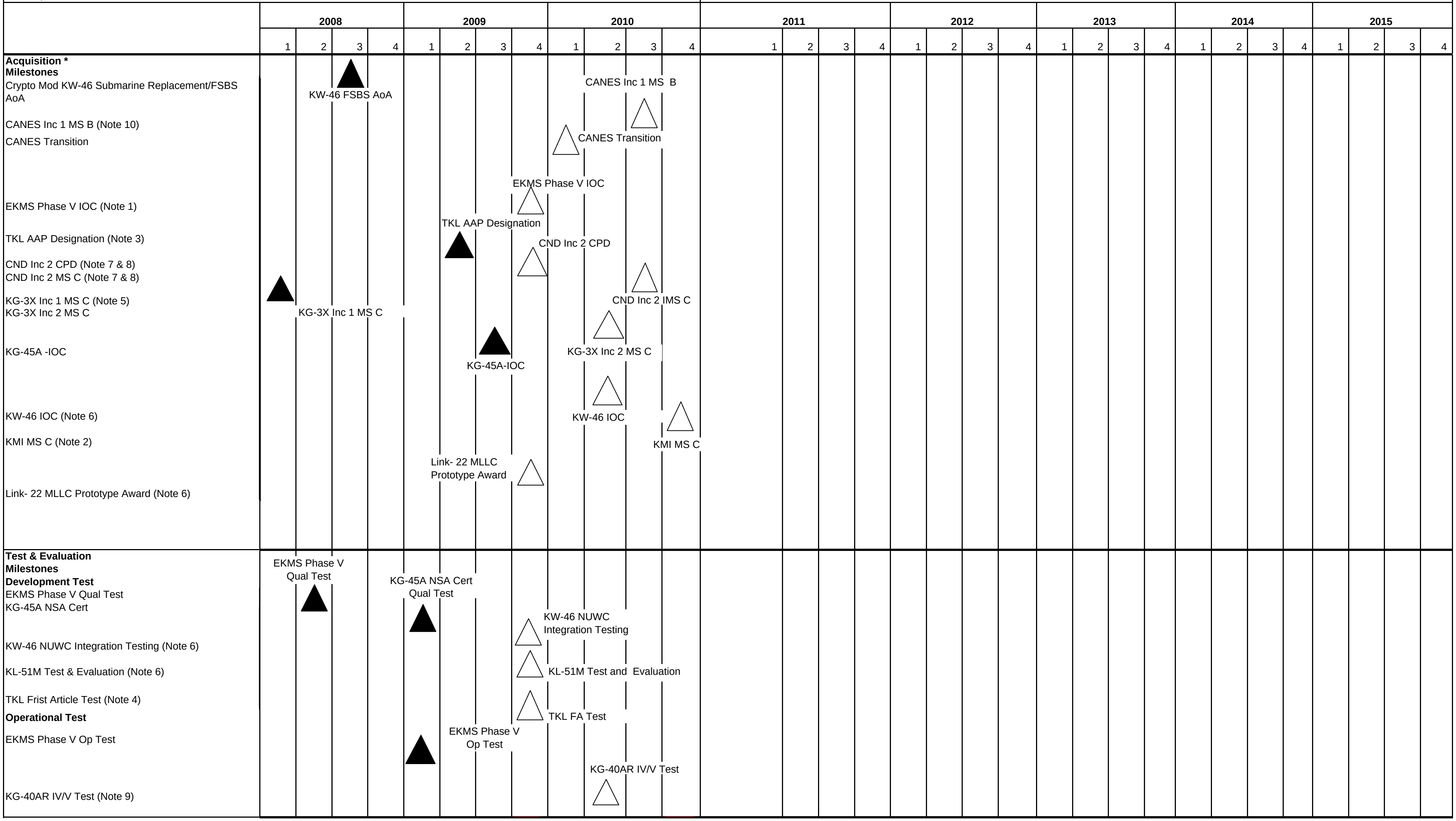
Exhibit R-3, Project Cost Analysis

Exhibit R-3 Cost Analysis (page 2)		**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E,N / BA-7	**PROGRAM ELEMENT** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 09 Cost	FY 09 Award Date	FY 10 Cost	FY 10 Award Date	FY 11 Cost	FY 11 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation	VAR	Various	30.271	4.357	VAR	0.495	VAR			Continuing	Continuing	Continuing
Subtotal T&E			30.271	4.357		0.495				Continuing	Continuing	Continuing
Remarks:												
Program Management Support	CPAF	Various	13.227	4.621	VAR	4.386	VAR			Continuing	Continuing	Continuing
Subtotal Management			13.227	4.621		4.386				Continuing	Continuing	Continuing
Remarks:												
Total Cost			266.275	24.820		22.026				Continuing	Continuing	Continuing
Remarks:												

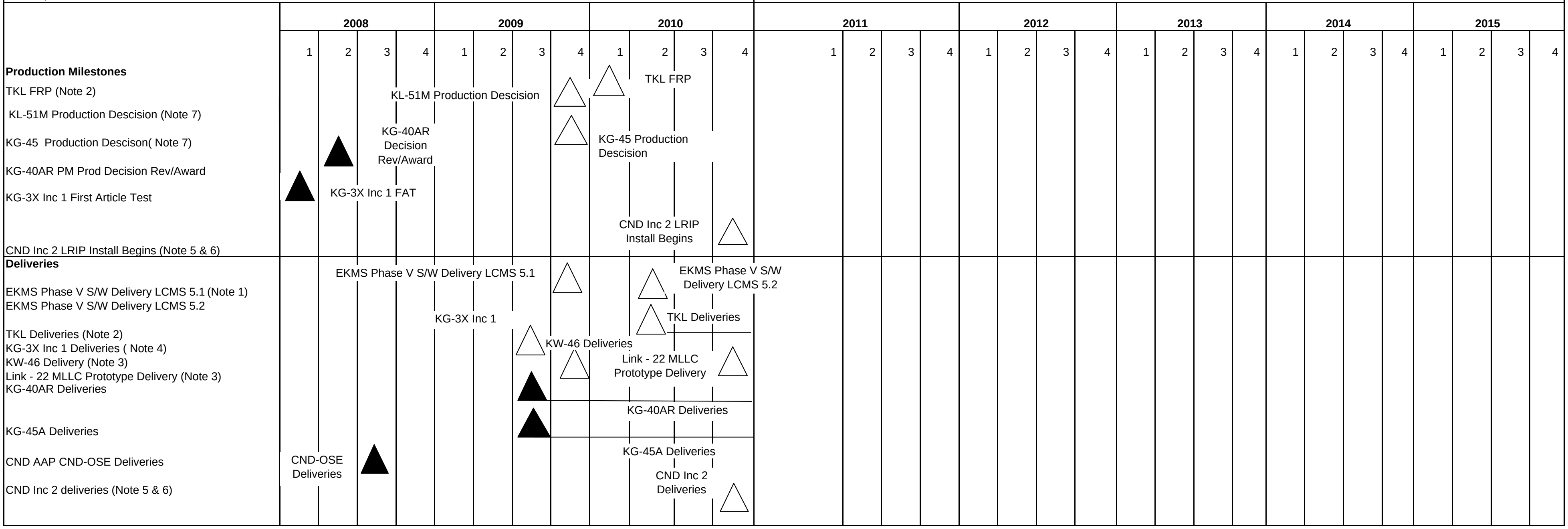
Exhibit R-3, Project Cost Analysis

EXHIBIT R4, Schedule Profile	**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY



Notes:
Note (1): EKMS Phase V IOC and delivery dates have continued to change as NSA schedule slips.
Note (2): KMI Milestone needed to reflect KMI objective schedule.
Note (3): TKL AAP designation approved 24 Mar 2009.
Note (4): TKL First Article Test, Production milestone, and delivery events not previously captured.
Note (5): Administrative change to record KG-3X Inc 1 MS C approval dated Jan. 2008.
Note (6): KW-46, Link 22 MLLC, KL-51M realignment of requirements not captured from previous submission.
Note (7): CND AAP established as Inc 1, with entry into Inc 2 post MS C authorized by ADM dated 13 Feb 2009.
Note (8): CND CPD was delayed to allow CPF (Commander, U.S. Pacific Fleet) time to resolve critical issues. The impact of this affects CND Inc 2 OT, LRIP installs, and deliveries.
Note (9): KG-40AR IV & V test & KG-45 production decision not captured from previous budget submission.
Note (10): Administrative change to record CANES Inc 1 MS B

EXHIBIT R4, Schedule Profile	**DATE:** May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROJECT NUMBER AND NAME** 0734 INFORMATION SYSTEMS SECURITY



Notes:
Note (1): EKMS Phase V IOC and delivery dates have continued to change as NSA schedule slips.
Note (2): TKL First Article Test, Production milestone, and delivery events not previously captured.
Note (3): KW-46, Link 22 MLLC, KL-51M realignment of requirements not captured from previous submission.
Note (4): KG-3X Inc 1 deliveries not previously captured.
Note (5): CND AAP established as Inc 1, with entry into Inc 2 post MS C authorized by ADM dated 13 Feb 2009.
Note (6): CND CPD was delayed to allow CPF (Commander, U.S. Pacific Fleet) time to resolve critical issues. The delay affects CND Inc 2 OT, LRIP installs, and deliveries.
Note (7): KG-40AR IV & V test, KG-45, KL-51M production decision not captured from previous budget submission.

Exhibit R-4a, Schedule Detail				DATE: May 2009				
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)			PROJECT NUMBER AND NAME 0734 INFORMATION SYSTEMS SECURITY				
Schedule Profile	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Crypto Modernization KW-46 FSBS AoA	3Q							
CANES Transition			1Q					
CANES Inc 1 MC B			3Q					
EKMS Phase V IOC (Note 1)		4Q						
TKL AAP Designation(Note 3)		2Q						
CND Inc 2 CPD (Note 8 and 9)		4Q						
CND Inc 2 MS C (Note 8 & 9)			3Q					
KG-3X Inc 1 MS C (Note5)	1Q							
KG-3X Inc 2 MS C			2Q					
KG-45A-IOC		3Q						
KW-46 IOC (Note 6)			2Q					
KMI MS C (Note 2)			4Q					
Link 22 MLLC Prototype Award (Note 6)		4Q						
Developmental Test								
EKMS Phase V Qualification Test	2Q							
Crypto KG-45A NSA Cert		1Q						
KW-46 NUWC Integration Testing (Note 5)		4Q						
KL-51M Test & Evaluation (Note 6)		4Q						
TKL FA Test (Note 4)		4Q						
KG-40AR IV/V Test (Note 10)			2Q					
Operational Test								
EKMS Phase V Operational Test		1Q						
Production Milestones								
TKL FRP (Note 4)			1Q					
KL-51M Production Decision (Note 10)		4Q						
KG-45 Production Decision (Note 10)		4Q						
KG-40AR PM Prod Decision Rev/Award	2Q							
KG-3X Inc 1 First Articles	1Q							
CND Inc 2 LRIP Installs Begin (Note 8 and 9)			4Q					
Deliveries								
EKMS Phase V S/W Delivery LCMS 5.1 (Note 1)		4Q						
EKMS Phase V S/W Delivery LCMS 5.2			2Q					
TKL Deliveries (Note 4)			2Q-4Q					
KG-3X Inc 1 Deliveries (Note 7)		3Q						
KG-40AR Deliveries		3Q-4Q	1Q-4Q					
KG-45 A Deliveries		3Q-4Q	1Q-4Q					
CND AAP CND-OSE Deliveries	3Q							
CND Inc 2 deliveries (Note 8 and 9)			4Q					

Exhibit R-4, Schedule Detail

Notes:

Note (1): EKMS Phase V IOC and delivery dates have continued to change as NSA schedule slips.
Note (2): KMI Milestone needed to reflect KMI objective schedule.
Note (3): TKL AAP designation approved 24 Mar 2008.
Note (4): TKL First Article Test, Production milestone, and delivery events not previously captured.
Note (5): Administrative change to record KG-3X Inc 1 MS C approval dated Jan. 2008.
Note (6): KW-46, Link 22 MLLC, KL-51M realignment of requirements not captured from previous submission.
Note (7): KG-3X Inc 1 deliveries not previously captured.
Note (8): CND AAP established as Inc 1, with entry into Inc 2 post MS C authorized by ADM dated 13 Feb 2009.
Note (9): CND CPD was delayed to allow CPF (Commander, U.S. Pacific Fleet) time to resolve critical issues. This delay affects CND Inc 2 OT, LRIP installs, and deliveries.
Note (10): KG-40AR IV & V test & KG-45 production decision not captured from previous budget submission.

EXHIBIT R-2a, RDT&E Project Justification						**DATE:** May 2009		
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)				**PROJECT NUMBER AND NAME** R0734/R3230/ONR BSO 14			
COST ($ in Millions)	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
Project Cost - R0734	**2.121**	**2.137**	**0.000**					
Project Cost - R3230	**0.000**	**0.000**	**2.200**					
RDT&E Articles Qty								

(U) A. MISSION DESCRIPTION AND BUDGET ITEM JUSTIFICATION:

The goal of the Navy Information Systems Security Program (ISSP) is to ensure the continued protection of Navy and Joint information and information systems from hostile exploitation and attack. ISSP activities address the triad of Defense Information Operations: protection, detection, and reaction. Evolving attack sensing (detection), warning, and response (reaction) responsibilities extend far beyond the traditional ISSP role in protection or Information Systems Security (INFOSEC). Focused on the highly mobile forward-deployed subscriber, the US Navy’s adoption of Network-Centric Warfare (NCW) places demands upon the ISSP, as the number of users explodes and the criticality of their use escalates. Today, the ISSP protects an expanding core of services critical to the effective performance of the Navy’s mission.

The rapid rate of change in the underlying commercial and government information infrastructures makes the provision of security an increasingly complex and dynamic problem. Information Assurance (IA) technology mix and deployment strategies must evolve quickly to meet rapidly evolving threats and vulnerabilities. The ISSP enables the Navy’s war fighter to trust in the availability, integrity, authentication, privacy, and non-repudiation of information.

This project includes funds for advanced technology development, test and evaluation of naval information systems security based on leading edge technologies that will improve information assurance (e.g., situational awareness and information infrastructure protection) across all Command echelons to tactical units afloat and war fighters ashore. This effort will provide the research to develop a secure seamless interoperable, common operational environment of networked information systems in the battle space and for monitoring and protecting the information infrastructure from malicious activities. This effort will provide Naval Forces a secure capability and basis in its achievement of protection from unauthorized access and misuse, and optimized IA resource allocations in the information battle space. This program will also develop core technology to improve network infrastructure resistance and resiliency to attacks; enable the rapid development and certification of security-aware applications and information technologies in accordance with the Common Criteria for IA and IA-Enabled information technology products by the National Security Telecommunications and Information Systems Security Instructions; and measure the effectiveness and efficiency of IA defensive capabilities under Naval environments.

The program will develop common architectural frameworks that facilitate integration of network security capabilities, enable effective seamless interoperation, and contribute to a common consistent picture of the networked environment with respect to information assurance and security. This effort will address the need for a common operational picture for Information Assurance (IA), as well as assessment of security technology critical to the success of the mission. Initiate requirements definition for situation awareness capabilities to support computer network defense in highly distributed, homogeneous, and heterogeneous networks including mobile and embedded networked devices. This effort also includes the architectural definition of situational awareness and visualization capabilities to support active computer network defense and support underlying data mining and correlation tools. This includes addressing the capability to remotely manage and securely control the configurations of network security components to implement changes in real time or near real time. Initiate requirements definition for secure coalition data exchange and interoperation among security levels and classifications. Ensure approaches address various security level technologies as well as emerging architectural methods of providing interoperability across different security levels. Examine multi-level aware applications and technologies including databases, web browsers, routers/switches, etc. Initiate infrastructure protection efforts as the Navy develops network centric architectures and warfare concepts, ensuring an evolutionary development of security architectures and products for IA that addresses Navy infrastructure requirements. Ensure the architectures evolve to provide proper protection as technology, DoD missions, and the threat all evolve. Include defensive protections as well as intrusion monitoring (sensors), warning mechanisms, and response capabilities in the architecture. Ensure the unique security and performance requirements of tactical systems, including those operating various security levels are addressed. Initiate the efforts to conceptualize new network centric warfare technology to protect our assets, such as secure network gateways and routers, and components and tools that improve the survivability of Navy networks. Provide systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

JUSTIFICATION FOR BUDGET ACTIVITY: This program is funded under OPERATIONAL SYSTEMS DEVELOPMENT because it encompasses engineering and manufacturing development for upgrade of existing, operational systems.

EXHIBIT R-2a, RDT&E Project Justification		**DATE:** May 2009	
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP	**PROJECT NUMBER AND NAME** R0734/R3230/ONR BSO 14	

(U) B. Accomplishments/Planned Program

	FY 2008	FY 2009	FY 2010	FY 2011
Software and Systems Research R0734	2.121	2.137	0.000	
Software and Systems Research R3230	0.000	0.000	2.200	
RDT&E Articles Quantity				

FY08: Continued working with commercial wireless technology to meet high assurance requirements, with particular emphasis on Navy and Marine Corps network centric environments. Initiated the development of wireless technology to augment the security posture of the commercial wireless technology. Continued the development of an information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Within the architecture/infrastructure, enhanced the framework to provide on-demand security services that supported confidentiality, integrity and authentication across security domains, as well as enforced the mission security policy. Completed development and refinement of infrastructure protection and architectures for Navy network centric architectures and warfare concepts. Ensured the architectures evolved to provide proper protection as technology, DoD missions, and the threat all evolve. Included improved defensive protections and response capabilities in the architecture, as well as provided support for traditional intrusion monitoring (sensors) and warning mechanisms. Developed technology and/or tools to ensure the unique security and performance requirements of tactical systems, including those operating at various security levels are addressed. Completed systems security engineering, certification and accreditation support for high-confidence naval information system and ensured certification and accreditation approaches were consistent with Navy and DoD requirements.

FY09: Complete the development of the wireless technology to meet high assurance requirements. Place the technology in selected Navy and Marine Corps sites for assessment. Use the feedback to improve the capabilities of the technology to better meet the mission requirements. Continue the development of an information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluate the security services of the framework that support confidentiality, integrity and authentication across security domains, as well as enforces the mission security policy. Use the assessment and operational feedback to improve the framework and security services. Enhance the framework to address survivability and hardening. Develop technology that protects the framework from attacks, assesses the attack, and responds appropriately to enable the framework to reconstitute and provide the requisite capabilities/services. Ensure the architecture/framework evolves to provide proper protection as technology, DoD missions, and the threat all evolve. Initiate development of modernized attack sensing and warning mechanisms based on new algorithms and data mining concepts, and response capabilities for the architecture/framework. Continue the development of technology and tools to ensure the unique security and performance requirements of tactical systems, including those operating at various security levels are addressed. Begin assessing the tools and technology in representative operational environments. Use the feedback to improve the tools and technology. Continue systems security engineering, certification and accreditation support for high-confidence naval information system and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

FY10: Complete the development of the information sharing architecture that addresses data integrity, confidentiality and policy management throughout networks of varying classification levels. Evaluate the security services of the architecture and adjust to ensure mission operations are supported. Continue the development of technology that protects, assesses and responds to attacks of the infrastructure architecture and provide reconstitution capabilities/services. Continue the development of modernized attack sensing and warning mechanisms based on new detection algorithms and data mining concepts, and response capabilities for the architecture. Complete the development of technology and tools to ensure the unique security and performance requirements of tactical wireless communication systems are addressed. Initiate the development of a new high assurance boundary controller to protect Navy and Marine Corps data and resources from attack. Provide security services including encryption and data malware analysis in the boundary controller. Initiate the development of a high-assurance computing environment for Navy and Marine Corps use based on trusted platform technology. Develop the appropriate core code, security messages and assurance functions required. Initiate the development of new key and enabling technologies, management tools, and capabilities to address specific Navy and Marine Corps needs. Ensure the new solutions address distribution and management of data and other requisite material. Continue systems security engineering, certification and accreditation support for high-confidence naval information systems and ensure certification and accreditation approaches are consistent with Navy and DoD requirements.

EXHIBIT R-2a, RDT&E Project Justification		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY RDT&E, N / BA-7	PROGRAM ELEMENT NUMBER AND NAME 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME R0734/R3230 COMMUNICATIONS SECURITY(INFORMATION ASSURANCE)

(U) C. OTHER PROGRAM FUNDING SUMMARY:

Line Item No. & Name	FY 2008	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015
OPN 3415 Info Sys Security Program (ISSP)	121.319	100.855	119.054					

(U) D. ACQUISITION STRATEGY:

N/A.

Exhibit R-2a, RDTEN Budget Item Justification

Exhibit R-3, Code Analysis (page 1)	**DATE:** May 2009	
APPROPRIATION/BUDGET ACTIVITY RDT&E,N / BA-7	**PROGRAM ELEMENT** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** R0734/R3230 COMMUNICATIONS SECURITY(INFORMATION ASSURANCE

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 09 Cost	FY 09 Award Date	FY 10 Cost	FY 10 Award Date	FY 11 Cost	FY 11 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Hardware Development												
Subtotal Product Developr			0.000	0.000		0.000				0.000	0.000	
Remarks:												
Software Development	WX	NRL, Washington, D.C.	10.777	2.137	11/09	2.200	11/08			Continuing	Continuing	
Subtotal Support			10.777	2.137		2.200				Continuing	Continuing	

Remarks:

Note: FY08-FY09 Figures reflect R0734 Communications Security. For FY10 they transition from Communications Security to Information Assurance.

Exhibit R-3, Project Cost Analysis

Exhibit R-3, Code Analysis (page 1)		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY **RDT&E,N / BA-7**	PROGRAM ELEMENT 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (IS	PROJECT NUMBER AND NAME R0734/R3230 COMMUNICATIONS SECURITY(INFORMATION ASSURANC

Cost Categories	Contract Method & Type	Performing Activity & Location	Total PY s Cost	FY 09 Cost	FY 09 Award Date	FY 10 Cost	FY 10 Award Date	FY 11 Cost	FY 11 Award Date	Cost to Complete	Total Cost	Target Value of Contract
Developmental Test & Evaluation												
Subtotal T&E			0.000	0.000		0.000				0.000	0.000	
Remarks:												
Program Management Support												
Subtotal Management			0.000	0.000		0.000				0.000	0.000	
Remarks:												
Total Cost			10.777	2.137		2.200				Continuing	Continuing	

Remarks:

Note: FY08-FY09 Figures reflect R0734 Communications Security. For FY10 they transition from Communications Security to Information Assurance.

Exhibit R-3, Project Cost Analysis

EXHIBIT R-2a, RDT&E Project Justification		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	PROJECT NUMBER AND NAME 9999 CONGRESSIONAL INCREASES

(U) B. Accomplishments/Planned Program

	FY 08	FY 09	FY 10	FY 11
9A99A Tactical Key Loader	3.092	0.000	0.000	
RDT&E Articles Quantity				

FY08: Tactical Key Loader: Established the TKL as an Abbreviated Acquisition Program. 1) System specification and design, 2) Hardware specification, design, and development of hardware mockups and breadboards, 3) Software specification, design, and development, and 4) Security specification, design, and input into the hardware and software development efforts. 5) Completed Build TKL test and evaluation laboratory with laboratory space provided by SPAWARSYSCEN San Diego (SSC-SD).

Exhibit R-2a, RDTEN Budget Item Justification

EXHIBIT R-2a, RDT&E Project Justification		DATE: May 2009
APPROPRIATION/BUDGET ACTIVITY **RDT&E, N / BA-7**	**PROGRAM ELEMENT NUMBER AND NAME** 0303140N INFORMATION SYSTEMS SECURITY PROGRAM (ISSP)	**PROJECT NUMBER AND NAME** 9999 CONGRESSIONAL INCREASES

(U) B. Accomplishments/Planned Program

	FY 08	FY 09	FY 10	FY 11
9B00A Universal Description, Discovery, and Integration	2.712	4.288	0.000	
RDT&E Articles Quantity				

FY08: Universal Description, Discovery, and Integration: Completed systems development of a demonstrable prototype that allowed users to discover and access valuable information at the right time based on the user's access clearance and need to know. Efforts also included support for Semantic services based on OWL-S and ebXML, Machine-to-Machine interfaces, and support to bridge OWL-S and WSDL based services. A trusted discovery service ensured that information accessed was at the appropriate level, provided the requisite information and prevented extraneous or unauthorized inputs and access. The web architecture-based solution allowed the user to access this information at the Navy enterprise level and eliminated the need to reconfigure networks and hardware when accessing one domain or another.

In order to implement a fully enabled end-to-end network enterprise environment envisioned Net-Centric Operations, completed the development of a component-based architecture called Secure Universal Description, Discovery, and Integration (UDDI). Secure UDDI provided the necessary components to meet the Naval warfighter requirements for both WSDL and OWL-S based services.

(1) Secure and non-reputable repository of services and information based on current open standards such as UDDI V3 and OWL-S.
(2) Incorporation of NSA certified components for authentication and authorization.
(3) Secure discovery of services and information.

FY09: Universal Description, Discovery, and Integration: Continue systems engineering to cover continued interoperability requirements for the architecture which demand a common security model to be established. Continue engineering implementation and warfighter/military utility assessment, risk reduction, and operational demonstration. Implement a prototype trusted discovery technology to demonstrate capabilites for integration in a high security, service orientated architecture environment. Begin development of software design, functional and security test plans.

	FY 08	FY 09	FY 10	FY 11
9E24A Trans Enterprise Services Grid (TSG) Technology Accreditation (TA	0.000	2.394	0.000	0.000
RDT&E Articles Quantity				

FY09: Trans Enterprise Services Grid (TSG) Technology Accreditation (TA): To develop a capability within PEO C4I / PMW160 / Information Systems Security Program's (ISSP) Computer Network Defense (CND) program. This work will focus on the Vulnerability Remediation Asset Management (VRAM) program and effectively sending and receiving Secure Configuration Compliance Validation Initiative (SCCVI) data generated by Retina scans between the ship and Fleet Numeric Mission Operations Center (FNMOC) facility and receiving information back when applicable.
Currently, this process requires the manual intervention of shipboard personnel to collect system scan data, manually initiate a transfer of that data to the FNMOC facility, observe that transaction, manually flush the system of data in cases of failed attempts, ensure the mitigation of any orphaned data in flight during loss of network connection, manually restart the transfer of data, manually confirm the reciept of said data shoreside, and manually log the transaction for post audit purposes. This process consumes far more human attention and intervention than desired due to the fragile nature of afloat network connectivity and frequent disconnections.
Initial efforts will seek to leverage the lessons learned throughout the SLAIN Small Business Innovative Research (SBIR) effort, along with complementary research and development efforts undertaken separately, to develop, accredit, and deploy VRAM enhancements that will provide the following four capabilities:

- Data persistence during the transfer of information
- Guaranteed delivery of VRAM data from ship to shore
- Provide an automated confirmation message to shipboard personnel that the scan data delivered successfully
- Reporting to be defined during development