Inspector General

United States Department of Defense

Inspections and Evaluations Directorate

Evaluation of Defense Installation Vulnerability Assessments

May 23, 2006
Report No. IE-2006.002

DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL

MISSION STATEMENT

The Office of the Inspector General promotes integrity, accountability, and improvement of Department of Defense personnel, programs and operations to support the Department's mission and to serve the public interest.

On the Cover:
We have chosen the Statue of Freedom from the United States Capitol as a symbol to be reflected in our report covers.

The bronze Statue of Freedom was designed by American sculptor Thomas Crawford in 1857-1859. Crawford described his creation as being readily understandable by the American people:

> *I have endeavored to represent Freedom triumphant — in Peace and War… In her left hand she holds the olive branch while the right hand rests on a sword which sustains the Shield of the United States. These emblems are such as the mass of our people will easily understand… I have introduced a base surrounded by wreaths indicative of the rewards Freedom is ready to bestow…*

Allen, William C., *The Dome of the United States Capitol: An Architectural History.* Prepared under the Direction of George M. White, FAIA, Architect of the Capitol, U.S. Government Printing Office Washington: 1992

If you suspect Fraud, Waste, Abuse, or Mismanagement in the Department of Defense, please contact us.
Phone: 800.424.9098 E-mail: hotline@dodig.mil Web site: www.dodig.mil/hotline

Evaluation of Defense Installation Vulnerability Assessments

May 23, 2006

Inspections & Evaluations
A Crystal Focus Review

VISION

A professional team of outcome-oriented inspectors promoting positive change by identifying opportunities for performance and efficiency improvements in Department programs and operations.

MISSION

The Directorate of Inspections and Evaluations conducts objective and independent customer-focused management and program inspections addressing areas of interest to Congress and the Department of Defense, and provides timely findings and recommendations leading to positive changes in programs.

Who Should Read This Report and Why?

This report should be read by military and civilian managers throughout the Department of Defense who have responsibility for developing, coordinating, or implementing policy or practices relating to organizing, resourcing, or assessing the Defense Critical Infrastructure Protection program. The report documents observations and recommendations of our program evaluation and summarizes resulting management actions.

What Was Identified?

Doctrine and organization changes driven by the Global War on Terrorism were incomplete. *Protection* and *assurance* concepts were disjointed, and coordination of associated programs could be improved. Through its Full Spectrum Integrated Vulnerability Assessment effort, the Office of the Assistant Secretary of Defense for Homeland Defense was attempting to address a significant part of this problem. This effort required coordination between multiple staff elements within the Office of the Secretary of Defense.

How It Could Be Improved?

We recommended that the Assistant Secretary of Defense for Homeland Defense should clearly decouple unique Defense Critical Infrastructure Protection efforts from Full Spectrum Integrated Vulnerability Assessment development. The success of the Defense Critical Infrastructure Protection program should not depend on a larger program integration effort.

Progress Review.

Our February 2005 briefing to the Assistant Secretary of Defense for Homeland Defense generated decisions and staff direction. As of November 2005, the Office of the Assistant Secretary of Defense for Homeland Defense had improved many aspects of the Defense Critical Infrastructure Protection program. Our recommendations caused or influenced the following actions.

- The Joint Staff J3, Deputy Director for Antiterrorism and Homeland Defense proposed changing the definition of force protection to include all hazards. The Director, Defense CIP amended the definition of "mission assurance" and included it in DoD Directive 3020.40.
- Defense CIP program officials chose preparedness as the concept overarching mission assurance and force protection. Acceptance of mission assurance as a complementary concept to force protection was increasing. The National Guard and the Defense Contract Management Agency demonstrated significant progress assessing non-DoD critical assets. Program officials worked with other OSD offices to realign responsibilities to reduce identified gaps and overlaps.
- The Assistant Secretary of Defense for Homeland Defense needed to complete the development of program policy and assessment standards that address all assets critical to DoD missions.
- The Assistant Secretary of Defense for Homeland Defense published interim threat, vulnerability, and criticality standards. His Principal Deputy established a field activity combining program management for Continuity of Operations, Continuity of Government, and Defense CIP.
- The Assistant Secretary of Defense for Homeland Defense actively pursued implementation funding and controlled Defense CIP funding within the Program Operating Memorandum in a discrete program element.

Much remains to be done as the program matures and continues to change in response to current events.

GENERAL INFORMATION

Forward questions or comments concerning the evaluation of Defense Installation Vulnerability Assessments and other activities conducted by the Inspections & Evaluations Directorate to:

Inspections & Evaluations Directorate
Office of the Deputy Inspector General for Policy & Oversight
Office of Inspector General of the Department of Defense
400 Army Navy Drive
Arlington, Virginia 22202-4704
crystalfocus@dodig.mil

An overview of the Department of Defense Office of Inspector General mission and organizational structure is available at http://www.dodig.mil.

TO REPORT FRAUD, WASTE, AND ABUSE

Contact the DoD OIG Hotline by telephone at (800) 424-9098, by e-mail at **hotline@dodig.mil** or in writing:

Defense Hotline
The Pentagon
Washington, D.C. 20301-1900

REPORT TRANSMITTAL

We are providing this report for information and use. We considered management comments to our findings in preparing this final report. Assistant Secretary of Defense for Homeland Defense comments conformed to the requirements of DoD Directive 7650.3, "Follow-up on General Accounting Office (GAO), DoD Inspector General (DoD IG), and Internal Audit Reports," June 3, 2004; therefore, additional comments are not required.

We also forwarded this report, as required by DoD Directive 7650.3, to the Audit Followup Directorate. The evaluation team included the results of a progress review in this report. We considered management actions acceptable and all recommendations closed. We did not request additional action.

Wm Brem Morrison, III
Assistant Inspector General
for Inspections and Evaluations

TABLE OF CONTENTS

List of Appendixes

This Page Intentionally Left Blank

Executive Summary

Defense Installation Vulnerability Assessments

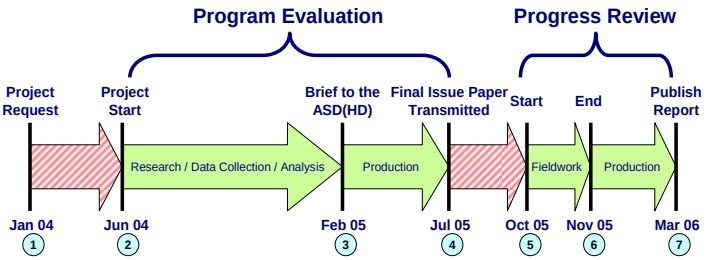
Background: In response to terrorist events, potential threats, and the increasing reliance on evolving information infrastructure, the Administration established a commission on national CIP in July 1996. The attacks of September 11, 2001 caused a major programmatic shift toward the protection of physical assets, especially in the continental United States (CONUS). At the national level, Congress established the Department of Homeland Security and assigned responsibility for national CIP to the new department. Homeland Security Presidential Directive 7 outlined the national CIP program and tasked DoD with responsibility for the Defense Industrial Base. The Secretary of Defense established U.S. Northern Command in February 2003 and the Office of the ASD(HD) in May 2003. In September 2003, the Deputy Secretary of Defense transferred Defense CIP oversight to the ASD(HD). While making significant changes to the program, the ASD(HD) recognized the value of an independent review and requested this evaluation. We initiated this project on June 17, 2004.

Evaluation Objective: Our objective was to evaluate policy and process for performing vulnerability assessments associated with Defense CIP, to include the Defense Industrial Base. Specifically we:

- evaluated proposed Defense CIP policy and program organization for Defense and non-Defense assets; and
- reviewed the effectiveness of the conduct of vulnerability assessments of Defense activities.

Early Implementation Review: In this review we assessed vulnerabilities, challenges, and successes of a new program during the start-up period. The Office of the Assistant Secretary of Defense for Homeland Defense [ASD(HD)] was a new office having recently received responsibility for Defense Critical Infrastructure Protection (CIP). Our priority for this review was to provide timely findings and recommendations focused on overall program effectiveness.

Figure 1. Project Timeline



1. Assistant Secretary of Defense for Homeland Defense requested the project.
2. Program Evaluation started based on the availability of resources.
3. We briefed program evaluation results to the Assistant Secretary (requestor).
4. We provided Issue papers to program management as we completed them.
5. We began the progress review.
6. We completed data collection on program progress.
7. We distributed program evaluation and progress review results.

Context: This report collates products provided directly to officials with responsibility for the Defense CIP program. We conducted the review in two primary phases (Program Evaluation and Progress Review) as shown in Figure 1.

We provided a summary of our program evaluation findings to the ASD(HD) on February 17, 2005. Subsequently, we provided the Director, Defense CIP with a detailed discussion of each identified issue and our recommendations. We began the progress review in October 2005 after allowing 8 months for Defense CIP officials to implement our recommendations. Our results are presented in the Progress Review section.

Program Evaluation Results

Observations: During our fieldwork, we determined that program managers within the Office of the ASD(HD) established strategic goals for the Defense CIP program. These goals were:

- to make available Defense critical infrastructure as required;
- to identify, prioritize, assess, and assure that Defense critical infrastructure is managed as a comprehensive program;
- to remediate or mitigate, based on risk, vulnerabilities found in Defense critical infrastructure; and
- to ensure Defense CIP will complement other DoD programs and efforts.

In addition, program managers within the Office of the ASD(HD) had taken actions to improve the program. They:

- published program strategy, prepared draft policy, and conducted program assessments and gap analyses;
- increased staffing, reorganized responsibilities, and actively engaged stakeholders on multiple levels;
- proposed strategic concepts, developed common program definitions, and pursued systemic solutions; and
- gained control over program funding and recognized the need for continued advocacy within the planning, programming, budgeting, and execution system.

Based on our review of documentation and interviews with responsible officials, we identified five areas of stress in the program.

- Asset Location: DoD owned, used, and relied on assets located both within and outside the United States. Overseas presence and operations created bureaucratic and jurisdictional gaps and overlaps.
- Asset Ownership: DoD owned significant assets, but was dependent on many outside its control. Success of Department operations relied on other government agencies, the Defense Industrial Base, and assets owned by host nations.
- Program Nexus: The Services, combatant commands, and Defense sectors all had a different focus. The Services focused on assets they owned, primarily their installations. Combatant commanders focused on warfighting assets, primarily equipment and supplies. Lead agencies for the Defense sectors concentrated on a narrow range of nonwarfighting assets. Non-DoD assets received insufficient attention.

- Program Participation: Legal issues surrounding implementation of Defense CIP at non-DoD organizations were not resolved. In addition, the role of the National Guard was unclear.
- Threats Addressed: Policy developed over time addressed the human threat, primarily in response to terrorist events including the bombing of Khobar Towers, the U.S.S. *Cole*, and the attacks of 9/11. However, as evidenced by the impacts of Hurricane Katrina, nonterrorist events can equal or exceed man-made impacts.

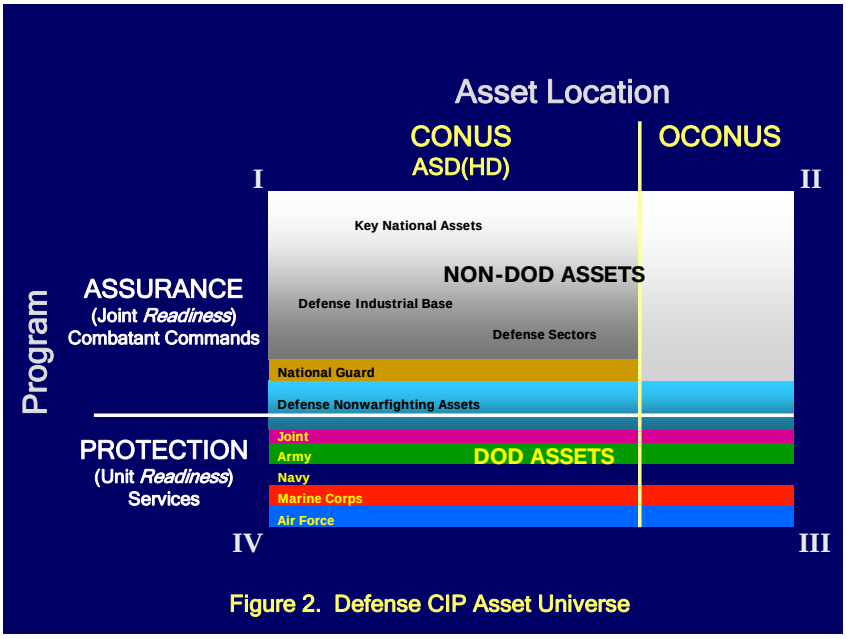


Figure 2. Defense CIP Asset Universe

Figure 2 illustrates the Defense CIP asset universe. The multicolored field proportionally represents all assets requiring Defense CIP criticality assessment, organized by asset ownership. The field is proportionally divided into four quadrants: vertically by geographic location and horizontally by predominant CIP-related readiness activity. In quadrants I and II, shading from dark to light reflects policy and implementation gaps, where white represents the absence of coverage. Assurance programs, including Defense CIP, are less developed. As shown in quadrants III and IV, protection programs provide relatively comprehensive coverage of DoD warfighting assets, including Service- and Joint-owned assets. Assurance program immaturity leaves gaps in the overall management of Defense nonwarfighting assets and non-DoD assets, especially assets located outside the continental United States (OCONUS).

Program Evaluation General Conclusion: Doctrine and organization changes were incomplete. The fundamental concepts defining protection and assurance were insufficiently developed and coordinated, and the division of roles and responsibilities among associated programs could be improved. Through their Full Spectrum Integrated Vulnerability Assessment effort, ASD(HD) attempted to address a significant part of this problem. However, the effort required coordination and integration of programs under the responsibility of multiple staff elements within the Office of the Secretary of Defense. Program officials should clearly separate specific Defense CIP efforts from Full Spectrum Integrated Vulnerability Assessment development.

Recommendations: We made six observations as a result of our evaluation, five of which included recommendations for improvement. We made no recommendation regarding our observation concerning stakeholder inclusion.

- Definitions. Responsible officials needed to update and complete definitions related to protection and assurance to incorporate current executive-level Homeland Security and CIP concepts.
- Responsibilities. The Office of the Under Secretary of Defense for Policy needed to reassign and modify protection and assurance program responsibilities to unify the programs under one overarching concept, increase attention to non-DoD assets critical to DoD missions, and rationalize the geographic overlap between subordinate offices.
- Assessment Standards. The ASD(HD) needed to complete the development of program policy and assessment standards that address all assets critical to DoD missions.
- Program Roles. The ASD(HD) needed to modify program responsibilities to include assigning the Joint Staff and combatant commanders management of warfighting assets and establishing a new Defense Field Activity to manage DoD nonwarfighting and non-DoD assets.
- Funding. The ASD(HD) needed to control program funding for program staff and support to stakeholders, obtain and allocate funding for vulnerability assessments, and advocate funding for mitigation of risk-based vulnerabilities.

Progress Review

Results: We conducted a progress review from October through November 2005. ASD(HD) developed and improved many aspects of the Defense CIP program following our debrief in February 2005.

- Definitions. Defense CIP officials in the office of the ASD(HD) published definition changes in agreement with our recommendations within DoD Directive 3020.40, but had not submitted changes for inclusion in Joint Publication 1-02.
- Responsibilities. Defense CIP program officials considered preparedness as the overarching concept for mission assurance and force protection. While acceptance of the concept of mission assurance was increasing, the Office of the Secretary of Defense had not yet fully accepted preparedness as the unifying construct.
- Assessment Standards. ASD(HD) had prepared draft guidance but still needed to develop consistent criticality methodology, threat communication processes, and vulnerability assessment standards for critical assets.
- Program Roles. ASD(HD) and the Defense Contract Management Agency had several ongoing initiatives addressing the Defense Industrial Base, but a lack of responsibility for assessment of non-DoD critical assets located OCONUS remained. The Principal Deputy Under Secretary of Defense for Policy approved the establishment of a field activity that will combine program management for Continuity of Operations, Continuity of Government, and Defense CIP.
- Funding. Finally, ASD(HD) established a program element to identify the Defense CIP implementation budget and planned to decentralize execution to the Services starting with the FY 2008 budget.

Introduction

Background

In response to terrorist events, including the bombing of the Khobar Towers, and the increasing reliance on evolving information infrastructure, the Administration established a commission on national Critical Infrastructure Protection in July 1996. Presidential Decision Directive No. 63, "Critical Infrastructure Protection" (PDD-63), May 22, 1998 (PDD-63), defined critical infrastructure as "physical and cyber-based systems essential to the minimum functions of the economy and government." PDD-63 also defined vulnerabilities, including "equipment failure, human error, weather and other natural causes, and physical and cyber attacks."

In response to PDD-63, DoD reissued DoD Directive 5160.54, "Critical Asset Assurance Program (CAAP)," January 20, 1998. DoD Directive 5160.54 expanded the requirement to identify, analyze, assess, and assure critical assets across the full range of military operations. However, the anticipated calendar year 2000 (Y2K) software problem focused national CIP program efforts during 1998 and 1999 on preventing cyber attacks to ensure the continuity and viability of critical information systems in the United States. DoD also reissued DoD Directive 2000.12, "DoD Antiterrorism/Force Protection (AT/FP) Program," April 13, 1999. The language of DoD Directive 2000.12 concentrated on the protection of personnel and reflected the prevalent attitude that terrorism occurred outside the United States.

The attacks of September 11, 2001, caused a major programmatic shift toward the protection of physical assets, especially in the United States. At the national level, Congress established the Department of Homeland Security and assigned to that Department responsibility for national CIP. DoD was tasked specifically with responsibility for the Defense Industrial Base. Homeland Security Presidential Directive 7 outlined the national CIP program, and Directive 8 defined *national preparedness*. The Secretary of Defense established U.S. Northern Command in February 2003 and assigned it responsibility for force protection in CONUS. The Secretary of Defense established ASD(HD) in May 2003.

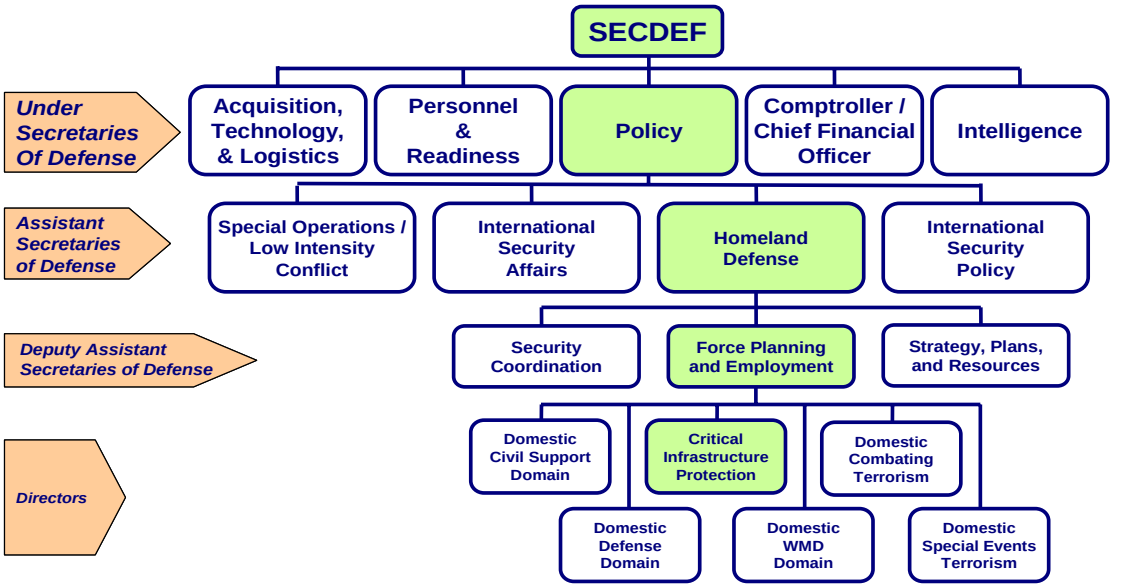
In September 2003, the Deputy Secretary of Defense transferred responsibility for Defense CIP oversight to the ASD(HD). Figure 2 below illustrates the location of Defense CIP in the Office of the Secretary of Defense. As of November 2005, Defense CIP was one of six programs under the responsibility of the Deputy Assistant Secretary of Defense for Force Planning and Employment. The Director, Defense CIP divided program responsibility among three deputies: Strategy and Policy, Operations, and Enterprise Architecture.

In September 2003, the Deputy Secretary of Defense realigned oversight of the Defense Critical Infrastructure Protection (CIP) Program to the Assistant Secretary of Defense for Homeland Defense (ASD[HD]). ASD(HD) primary Defense CIP responsibilities are to

- act as the principal staff assistant and civilian advisor to the Secretary;
- represent DoD with the Department of Homeland Security;

- prepare and present budget submissions to the Office of the Secretary of Defense (OSD);
- represent DoD before the U.S. Congress; and
- develop analytical standards and procedures to ensure effective analyses and assessments.

Figure 2. Defense CIP Organization



Objective

The ASD(HD) requested the Inspector General review implementation of the analytical standards and procedures. We initiated this project on June 17, 2004. Our overall objective was to evaluate policy and processes for performing vulnerability assessments associated with Defense CIP, to include the Defense Industrial Base. Specifically, we:

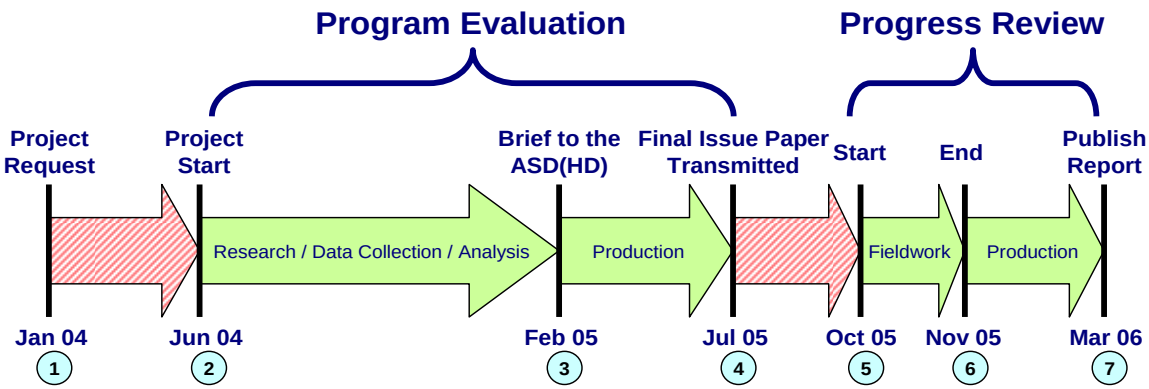
- evaluated proposed Defense CIP policy and program organization for Defense and non-Defense assets; and
- reviewed the effectiveness of the conduct of vulnerability assessments of Defense activities.

Early Implementation Review

We define an early implementation review as a study that assesses vulnerabilities, challenges, and successes of a new initiative or program during the start-up period. Although Defense CIP was not a new program, ASD(HD) was a new office that had recently received responsibility for the program. Program officials were new to their responsibilities and were making significant changes. Our priority for this review was to provide timely findings and recommendations focused on overall program effectiveness.

The remaining sections of this report collate the products provided directly to officials with responsibility for the Defense CIP program. We conducted the review in two primary phases (Program Evaluation and Progress Review) as shown in Figure 1.

Figure 1. Project Timeline



1. Assistant Secretary of Defense for Homeland Defense requested the project.
2. Program Evaluation started based on the availability of resources.
3. We briefed program evaluation results to the Assistant Secretary (requestor).
4. We provided Issue papers to program management as we completed them.
5. We began the progress review.
6. We completed data collection on program progress.
7. We distributed program evaluation and progress review results.

We conducted fieldwork for the program evaluation from June 2004 through February 2005. The objective of the evaluation was to assess policy and process for performing vulnerability assessments associated with Defense CIP. We provided a summary of our findings to the ASD(HD) on February 17, 2005 (see Appendix B). This was our primary product for the program evaluation phase. During the briefing we provided the ASD(HD) with five opportunities for program improvement and an overarching recommendation designed to provide sufficient information for executive decisions. Subsequently, we provided the Director, Defense CIP with a detailed discussion of each identified issue including our recommendations. One issue did not include recommendations; therefore, we provided no additional information beyond the briefing.

We began the progress review in October 2005, after allowing 8 months for Defense CIP officials to implement our recommendations. The progress review was designed to evaluate the value of our recommendations to program management, determine their implementation, and ascertain significant program changes. We interviewed Defense CIP program officials, the ASD(HD) Comptroller, and representatives with Defense CIP program responsibility in the Joint Staff and Defense Contract Management Agency. Our results are presented in the Progress Review section.

This Page Intentionally Left Blank

Issue 1. Definition Changes

The addition of the continental United States (CONUS) as a significant element to the Global War on Terrorism necessitated changes to DoD policy and organization. Attempts to establish policy, assign responsibility, and develop programs were hindered by the lack of generally accepted terminology to describe underlying concepts.

Discussion

The attacks of September 11, 2001, shifted the focus for prevention of further terrorist attacks to the homeland, and generated significant organizational change in the Federal Government. Homeland Security Presidential Directive No. 8, "National Preparedness," December 17, 2003, defines *all-hazards preparedness* and establishes a national domestic all-hazards preparedness goal. Directive No. 8 equates *preparedness* with *readiness* for the national program. Priorities within both the National and Defense CIP programs also shifted: although the security of cyber systems remained important, attention to the protection of physical assets increased. The two terms used by DoD to define the primary activities associated with Defense CIP, force *protection* and mission *assurance*, do not encompass all critical assets and potential threats.

As of February 2005, Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms," (JP 1-02) defined *force protection* as:

> Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

That definition does not address all aspects of CIP. The definition implies defensive action, is applicable only to DoD assets, and excludes important categories of threats. Effective CIP requires responsible officials to identify and protect all assets that allow them to perform essential missions, not just assets under their control.

In addition, comprehensive force protection should address a greater range of threats. Directive No. 8 adopts an all-hazards approach, and Defense CIP policy recognizes all hazards. The impact of multiple hurricanes in

Florida and the earthquake and tsunami in the Indian Ocean in 2004 demonstrate the need for the all-hazards approach.

The term *mission assurance* is not listed in JP 1-02. In draft DoD Directive 3020.ff, "Defense Critical Infrastructure Program (DCIP)," October 2004, the Office of the Assistant Secretary of Defense for Homeland Defense proposed to define mission assurance as:

> A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy. It links numerous risk management program activities and security related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

The language of the draft is confusing, describing mission assurance alternately as an activity leading to readiness and as a necessary state for successful military operations. It lists readiness as a complementary or subordinate risk management or security-related function. However, DoD Directive 5160.54, "Critical Asset Assurance Program (CAAP)," January 20, 1998, clearly defines *assurance* as an activity. The proposed addition of the term *mission*, which has its own definition in JP 1-02, adds no value to the concept of assurance.

Even though the definition of force protection includes personnel, resources, facilities, and critical information, in general, force protection activities focus on personnel. For example, DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003, states that an explicit goal of the antiterrorism program is the protection of DoD elements and personnel. That program is one activity that addresses aspects of force protection. Also, DoD Instruction 2000.16, "DoD Antiterrorism Standards," June 14, 2001, specifically limits higher headquarters vulnerability assessments to installations with "300 or more personnel on a daily basis." The instruction allows for vulnerability assessments at any DoD facility if the appropriate commander identifies a need. Antiterrorism policy should require assessments at facilities that are deemed critical under CIP standards, regardless of the number of personnel impacted, to help integrate activities and mitigate risk.

Impact

CIP program managers have been unable to complete coordination and publication of program policies. The lack of concise or generally accepted terminology describing concepts and doctrine has caused several stakeholders to nonconcur with draft directives. Obsolete or missing DoD policy hindered program implementation and execution, and made funding difficult to obtain. Clear definitions and concepts will allow for efficient distribution of program responsibilities and help prevent overlaps and gaps in protection and assurance activities.

Recommendations

We recommended the Assistant Secretary of Defense for Homeland Defense should:

1. Request that the Director for Operational Plans and Joint Force Development, Joint Staff amend the term Force Protection in Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms," by deleting the word *force* and including an all-hazards component within that definition to ensure consistency with the intent of Homeland Security Presidential Directive No. 8.

2. Amend the term *mission assurance* in DoD Directive 3020.ff, "Defense Critical Infrastructure Program (DCIP)," October 2004, by deleting the word *mission*, and refining the definition to include specific policy considerations as set forth in DoD Directive 5160.54, "Critical Asset Assurance Program (CAAP)," January 20, 1998.

3. Request that the Director for Operational Plans and Joint Force Development, Joint Staff include the revised assurance definition in Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms."

Issue 2. Program Responsibilities

DoD preparedness concepts, including Defense CIP, were disjointed, and associated programs were inadequately coordinated.

Discussion

Homeland Security Presidential Directive No. 8, "National Preparedness," December 17, 2003, requires a national domestic all-hazards preparedness goal. Directive No. 8 defines *all-hazards preparedness*, and equates *preparedness* with *readiness* for the national program.

As of March 2005, Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms," (JP 1-02) defines readiness as:

> The ability of US military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels. a. unit readiness - The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. b. joint readiness - The combatant commander's ability to integrate and synchronize ready combat and support forces to execute his or her assigned missions.

Under this definition, all activities conducted by DoD components, other than Operations, contributed to readiness. General examples of these activities include acquisition, staffing, training, and logistical support. However, the two specific CIP activities contributing to readiness are *protection* and *assurance*.

Protection, which is defined in JP 1-02 as force protection, is an activity associated with unit readiness. As defined, protection actions are limited to the protection of DoD assets. Those actions seek to "preserve the force's fighting potential;" hence, these actions are generally defensive in nature. *Assurance*, defined in DoD Directive 5160.54, "Critical Asset Assurance Program (CAAP)," January 20, 1998, and draft DoD Directive 3020.ff, "Defense Critical Infrastructure Program (DCIP)," October 13, 2004, is an activity associated with *joint readiness*. Assurance actions are broader, designed to "ensure that required capabilities and all supporting structures are available to the DoD to carry out the National Military Strategy." Protection and assurance activities are complementary, and both contribute to different facets of readiness.

Civilian directors and military commanders at all levels performed protection and assurance activities through a variety of programs. However, responsibility for programs, as well as underlying protection

and assurance concepts, was spread across multiple Under and Assistant Secretaries of Defense, as shown in Table 1.

Table 1. Protection and Assurance Program Responsibility

PROGRAM	RESPONSIBLE OFFICE	COMMENTS
PROTECTION		
Antiterrorism	ASD(SO/LIC)	
Chemical, Biological, Radiological, Nuclear, and High-Explosives	ATSD(NCB), USD(AT&L), ASD(SO/LIC)	ATSD(NCB) responsible for Chemical, Biological, and Nuclear policy. Responsibility for radiological policy divided. Department of Defense Explosive Safety Board published conventional explosives standards. ASD(SO/LIC) drafting policy for emergency response.
Physical Security	USD(I)	
Installation Preparedness	ASD(SO/LIC), ASD(HD), USD(AT&L)	ASD(SO/LIC) drafting policy. ASD(HD) published the September 2003 report to Congress. USD(AT&L) responsible for the Joint Service Installation Preparedness Pilot and Unconventional Nuclear Warfare Defense programs.
ASSURANCE		
Continuity of Operations, Continuity of Government	USD(P)	
Information Assurance	ASD(NII)	
Critical Infrastructure Protection	ASD(HD)	

ACRONYM LIST

ASD(NII)	Assistant Secretary of Defense for Network Information and Integration
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
ATSD(NCB)	Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

Prior to September 11, 2001, no significant CONUS threat had been identified, and DoD focused protection and assurance activities OCONUS. The increased efforts for homeland security added a geographic element to the division of protection and assurance responsibilities. As of February 2005, the charter document outlining authorities and assigning responsibilities to the Office of the ASD(HD) remained in draft. However, the ASD(HD) defined his responsibility as the defense of "U.S. sovereignty, territory, domestic population, and critical infrastructure." Protection and assurance program responsibility was not realigned to match geographic limitations. ASD(HD) had global responsibility for Defense CIP, but had no direct responsibility for protection programs in CONUS. Effective CIP involves the assurance of all assets, both civilian and military, necessary to project, support, and sustain military forces worldwide.

The geographic division of responsibility is not unique to protection and assurance programs. For example, environmental legislation has limited extraterritorial application. In response, DoD developed effective parallel policy based on consistent environmental standards for use in CONUS and OCONUS. However, coordinating this effort was simplified because the Deputy Under Secretary of Defense for Installations and Environment has policy responsibility for the entire environmental program.

Impact

Disjointed and overlapping protection and assurance concepts resulted in inefficient implementation and unclear responsibility for the protection of assets. Program officials continued to expend time and effort attempting to agree on definitions, thus delaying the deployment of program capabilities. The ultimate result was the diffusion of civilian responsibility and confused authority. Without clear assignment of responsibilities, asset owners receive conflicting guidance, multiple assessments of assets, and uncoordinated funding for mitigation efforts.

Recommendations

We recommended the Office of the Under Secretary of Defense for Policy should:

1. Organize Protection and Assurance programs and initiatives under a common overarching concept to rationalize efforts toward all-hazards preparedness.

2. Complete DoD Directive 5111.13, “Assistant Secretary of Defense for Homeland Defense” and amend DoD Directive 5111.10, “Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SO/LIC)),” March 22, 1995, to reflect a geographic division of responsibility for Protection and Assurance policy and programs. CONUS, Alaska, Hawaii, and U.S. Territories and Protectorates should be assigned to the Assistant Secretary of Defense for Homeland Defense, and OCONUS should be assigned to the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.

Issue 3. Assessment Standards

As of February 2005, the Defense CIP program did not provide sufficient deployed capabilities. In addition, prioritizing efforts and applying program resources were not optimized to address nonwarfighting critical assets.

Discussion

Draft DoD Directive 3020.ff, "Defense Critical Infrastructure Program (DCIP)," October 13, 2004, defines Defense CIP as "a risk-based DoD program that seeks to assure the availability of infrastructures critical to DoD missions." It states that DoD will achieve this goal by identification, assessment, and security enhancement of assets essential for executing the National Military Strategy. As of February 2005, comprehensive assessment standards were incomplete, integrated assessments were not being performed, and program efforts assessing nonwarfighting assets were insufficient.

At the request of Defense CIP program officials, the Defense Program Office for Mission Assurance (DPO-MA) published the "Defense Critical Infrastructure Program: Full Spectrum Integrated Vulnerability Assessment Program Concept of Operations, Version 1.0," which states:

> This Concept of Operations (CONOPS) addresses the need for a Defense-wide, comprehensive, integrated, repeatable, and sustainable vulnerability assessment process in accordance with Defense Critical Infrastructure Program (DCIP) policy, as stated in draft DoD Directive (DoDD) 3020.ff. To accomplish this, the document outlines the functions and processes of the DCIP Full Spectrum Vulnerability Assessment Program and the organizations within DoD responsible for establishing and ensuring such assessments.

The document fails to identify the organizations responsible for conducting vulnerability assessments, stating only that assessment organizations must coordinate and execute Defense CIP Full Spectrum Integrated Vulnerability Assessment program requirements in accordance with this Concept of Operations and other applicable documentation.

In July 2004, DPO-MA published the "Full Spectrum Integrated Vulnerability Assessment Program Team Standards, Version 1.0," containing standards in 12 areas of concern. In the scope section, DPO-MA stated that the standards were applicable to "the assessment of all DoD critical assets, including non-DoD Federally-owned or leased critical assets and commercial critical assets that support the DoD mission."

The document was predominantly a compendium of then-current standards for assessing DoD assets. For example, the standards for assessing continuity of operations in the Plans area of concern and outer perimeter security in the Physical Security area of concern were derived from current standards applicable to Federal facilities. In two other areas of concern, Supporting Infrastructure Networks and Availability of Supporting Material and Services, DPO-MA established standards to determine vulnerability based on standards applicable to both Federal and non-Federal facilities. Further, the criteria were not designed to determine interdependency among critical assets, a vital Defense CIP concept. Inspectors using the standards as a guide will likely perform CIP assessments of critical DoD assets identical to and duplicative of other protection and assurance assessments. Moreover, inspectors will have difficulty conducting assessments on non-DoD assets because of lack of ownership and access.

As of March 2005, DPO-MA was still conducting pilot vulnerability assessments. These tests ran concurrently with Joint Service Integrated Vulnerability Assessments and Balanced Survivability Assessments, both conducted by the Defense Threat Reduction Agency as part of the antiterrorism program. DPO-MA intended the pilot assessments as tests of Full Spectrum Integrated Vulnerability Assessment protocols. They focused their efforts on integrating existing assessments and eliminating overlaps.

DPO-MA conducted 11 assessments in FY 2004 and Defense CIP program management planned 6 during FY 2005. All assessments were of DoD-owned facilities. Consequently DPO-MA did not examine critical National Guard or non-DoD assets. DoD warfighting assets on military installations were protected to a higher standard and assessed under multiple protection and assurance programs. The Defense CIP assessment plan did not address non-DoD assets, the areas of greatest weakness.

Defense CIP program officials accomplished significant progress in conducting DoD assessments, but applied insufficient attention to the specified mission of protecting the Defense Industrial Base. Homeland Security Presidential Directive No. 7 explicitly assigns responsibility to DoD for protection of the Defense Industrial Base. DoDD 3020.ff assigns the Defense Contract Management Agency as the lead agency for protection of the Defense Industrial Base within DoD. As of February 2005, CIP program responsibility within Defense Contract Management Agency was an additional duty performed at a relatively junior level. Further, according to senior officials, the Joint Staff assigned low priority to the protection of nonwarfighting critical assets.

Impact

The Defense CIP program did not adequately identify and protect infrastructures deemed critical for national security. Specifically, DoD's vulnerability to an event disrupting critical DoD nonwarfighting and non-DoD assets remained unknown. The mission impacts remain unidentified as well. More complete assessments are needed to effect appropriate prioritization and funding.

In addition, program management's inability to adequately define and assign assessment responsibilities created duplication of effort and confusion at installations receiving multiple findings and reports.

Recommendations

We recommended the Assistant Secretary of Defense for Homeland Defense should:

1. Complete Defense CIP assessment standards for non-DoD assets and unique CIP standards for DoD assets.

2. Integrate Defense CIP assessments that review non-DoD assets with assessments conducted on DoD assets.

3. Coordinate and fund "expert type" assessments for vital strategic DoD and non-DoD national assets.

4. Refocus CIP program activities to assure the availability of DoD nonwarfighting, National Guard, and non-DoD assets critical to DoD missions.

Issue 4. Program Roles

Defense CIP program organization was inadequate to achieve desired homeland defense strategic objectives.

Discussion

Homeland defense objectives relating to Defense CIP are outlined in three documents. First, Homeland Security Presidential Directive No. 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003, tasks all Federal departments to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them." Second, draft DoD Directive 3020.ff states program objectives which include:

> The identification, prioritization, assessment, and assurance of Defense Critical Infrastructures … managed as a comprehensive program that includes the development of adaptive plans and procedures to: mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect related information.

DoD Directive 3020.ff also defines critical infrastructures to include essential DoD and non-DoD assets worldwide. Third, in "DoD Strategy for Homeland Defense and Civil Support (Coordinating Draft)," September 13, 2004, the ASD(HD) listed DoD objectives and core capabilities for protecting the U.S. from attack. According to this strategy, an effective Defense CIP program must "implement a protective risk management strategy for defense critical infrastructure" and "conduct protection operations for designated national critical infrastructure." Once fully capable, the Defense CIP program will contribute to the objective of providing mission assurance.

The Director of Defense CIP has program responsibility within the office of the ASD(HD). The Director is responsible for developing and overseeing implementation of policy for worldwide identification, prioritization, assessment, remediation, and protection of critical infrastructure. However, the ASD(HD) area of responsibility was limited to the United States, Territories, and the approaches. Prior to the establishment of the Homeland Defense office, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict was responsible for policy and advice on the use of U.S. Government resources in counterterrorism and antiterrorism. The responsibility of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict was not geographically limited. Reaching consensus on the division of

responsibilities took time and absorbed effort that management could have applied to developing program capabilities.

As of February 2005, Defense CIP program officials were using the Defense Program Office for Mission Assurance for a wide variety of program management tasks. However, in October 2004, program officials proposed realigning Defense Program Office for Mission Assurance support and reducing staffing from 219 to 117 positions. The same proposal recommended supporting each of the 10 Defense sectors identified in DoD Directive 3020.ff with 3 full-time staff, a significant improvement. For example, as of September 2004, the Defense CIP working group responsible for the Defense Industrial Base identified over 1000 important and over 150 critical facilities, excluding overseas installations. The sector lead agency, the Defense Contract Management Agency, managed its own program using one GS-14 taken from existing staff.

The system for conducting assessments to identify vulnerabilities, prioritize impacts, and coordinate mitigation was in the initial phases of development. Assessment standards and protocols, databases and tracking tools, and mitigation activity prioritization were all in draft or test phase. Defense CIP program officials understood the need for a coordinated effort among protection and assurance programs involving multiple Under and Assistant Secretaries of Defense. However, their efforts to coordinate multiple programs detracted from the development of fundamental program structure.

Efficient accomplishment of homeland defense strategic objectives required coordination between protection and assurance programs. Coordination should culminate in systems that ensure consolidated, analyzed assessment information for all stakeholders. Different assessment groups need to use a common data set representing the facility or installation and apply an integrated, relevant threat picture. Using common baselines would encourage comparable results from different groups and minimize duplication and repetition.

Impact

Inadequate program structure resulted in inefficient application of resources, gaps in analysis, and unnecessary disruption at installations. Responsible offices need to retain some control of dedicated resources. However, fragmented protection and assurance efforts did not facilitate the application of a strategic vision that balanced all areas of program responsibility. Disjointed efforts led to insufficient review of

nonwarfighting assets under DoD responsibility and potential gaps in the analysis of national level assets and DoD-wide systems. Finally, the lack of a single program office or activity responsible for establishing standards and coordinating worldwide assessments created duplication and the perception of conflicts at installations. Installation representatives stated they received multiple assessments, often reviewing the same functional areas and systems, with many assessments producing repeat findings and inconsistent results (same system or function, different findings). Assigning a field activity to coordinate and track various protection and assurance efforts would permit more efficient execution of protection and assurance programs.

Recommendations

1. We recommended the Assistant Secretary of Defense for Homeland Defense should establish a field activity responsible for implementing and monitoring Department protection and assurance programs. The field activity should have the following primary responsibilities:

a. develop, validate, and accredit assessment and training standards for assessors;

b. standardize, consolidate, and archive facility infrastructure and vulnerability assessment data;

c. identify protection and assurance issues with broad impacts across nonwarfighting assets or DoD-wide applicability; and

d. obtain, integrate, and share relevant threat data with assessing organizations.

2. The Assistant Secretary of Defense for Homeland Defense should publish policy that assigns responsibility to:

a. conduct Defense Critical Infrastructure Protection program vulnerability assessments,

b. standardize definitions and criteria for determining asset criticality; and

c. develop quantifiable program metrics.

Issue 5. Program Funding

Defense CIP planning and programming was inadequate to reduce critical vulnerabilities.

Discussion

The realignment of Defense CIP oversight to the ASD(HD) did not resolve issues relating to programmatic funding. Officials responsible for implementing Defense CIP programs at command levels cited the lack of established policy addressing program and mitigation funding as a significant concern.

In 2002, the Defense Science Board Summer Study on Special Operations and Joint Forces in Support of Countering Terrorism recommended an "increase tenfold (over three years) [of] the people and resources devoted to assessing vulnerabilities of our DoD force protection capabilities and critical infrastructure." In the report, the Defense Science Board estimated assessment costs in excess of $100 million, and further estimated $150 million yearly requirement to redress vulnerabilities. The report also recommended that DoD establish a separate funding line for assessment and mitigation funding.

Prior to FY 2005, Defense CIP program funding was split between the ASD(HD) and the Joint Program Office (later the Defense Program Office) for Mission Assurance under the Department of the Navy. Budget authority for the FY 2005 Defense CIP program was consolidated under the ASD(HD) in two program elements: OSD Operations and Maintenance ($18 million), and CIP Research, Development, Testing, Evaluation ($22 million). Program officials stated that their priority for FY 2005 was the establishment of Defense CIP offices in combatant commands and Defense sectors, and that an additional $9 million was potentially available. However, budgeted amounts were well short of Defense Science Board recommendations.

Commands expressed frustration that Defense CIP emphasized the assessment concept without the concomitant emphasis on mitigating the vulnerabilities the assessments identified. Command and installation requests for Defense CIP mitigation funds competed with all other requirements through the regular Planning, Programming, Budgeting, and Execution (PPBE) process. As of February 2005, the Office of the ASD(HD) was not involved in mitigation funding or the disbursement of funds for that purpose, but representatives anticipated an increased role beginning with the FY 2007 budget.

The Combating Terrorism Readiness Initiatives Fund of the Antiterrorism program allows the Joint Staff to fund force protection mitigation against emerging threats. This program provides an example of efficient targeting of funds to prioritized projects. As of February 2005, the Defense CIP program had no comparable process, and commanders were not afforded access to Combating Terrorism Readiness Initiatives Funds to mitigate vulnerabilities unique to Defense CIP. Command representatives with responsibility for Defense CIP stated that programmatic inclusion in the PPBE system was necessary for continued program development.

Impact

A lack of stable funding for the Defense CIP program contributed to problems with program implementation throughout the combatant commands and Defense sectors. It was detrimental to long-term planning for vulnerability assessments. In addition, insufficient resources for mitigation of identified vulnerabilities led to frustration at installations. Defense CIP assessments highlighted problems, making commanders aware of weaknesses without providing a ready means for relief. Decentralized funding without centralized prioritization and oversight discouraged effective mitigation efforts. Determining which assets were critical depended on mission requirements that varied with level of command. Thus, a mitigation effort to protect an asset critical to a combatant commander could receive a low priority from an installation commander. Vulnerabilities that remained uncorrected increased the risk to mission assurance.

Recommendations

We recommended the Assistant Secretary of Defense for Homeland Defense should:

1. Establish the Critical Infrastructure Protection program in the planning, programming, budgeting, and execution system and control and coordinate program implementation funding.
2. Advocate for mitigation funding from a consolidated, prioritized database of risk-based vulnerabilities identified through a coordinated assessment process.

Evaluation Response to Management Comments

ASD(HD) concurred with the majority of our recommendations. We discuss specific instances of disagreement and potential impacts below. The following is a summary of the management comments and the OIG response. Full management comments can be found in Appendix B.

Issue 1. Definition Changes

ASD(HD) disagreed with our recommendation to shorten *mission assurance* to *assurance* and *force protection* to *protection*, but agreed with the need to include program definitions in the Joint Dictionary of Military and Associated Terms. The intent of the recommendation was to simplify and clarify fundamental concepts used to assign responsibility, establish policy, and define requirements. Management choosing not to support the change had no substantial impact on the Defense CIP program.

Issue 2. Program Responsibilities

ASD(HD) supported our recommendation to organize protection and assurance concepts under a common overarching concept. However, management chose to use the term *preparedness* instead of *readiness*. We proposed *readiness* specifically because it represented the military term best matching preparedness. Management's choice of *preparedness*, the term used in national policy, is acceptable. Also, ASD(HD) did not agree with our recommendation to divide responsibility for protection and assurance policy based on geographic areas of responsibility. We concur with management's analysis. The Under Secretary of Defense for Policy adjusted responsibilities between ASD(HD) and the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. However, officials need to codify their agreements in policy.

Issue 3. Assessment Standards

ASD(HD) disagreed with our recommendation to integrate Defense CIP assessments with Joint Staff Integrated Vulnerability Assessments. We concur with their analysis, which is based on a series of jointly conducted pilot assessments. Ensuring effective and comprehensive CIP assessments takes precedence over efficiency gains through integration with existing assessment programs.

Progress Review

We conducted a progress review from October through November 2005 to ascertain significant program changes and determine the impacts of our recommendations. Since our briefing to the ASD(HD) in February 2005, the office of the ASD(HD) further developed and improved many aspects of the Defense CIP program. The ASD(HD) published two important documents: "Strategy for Homeland Defense and Civil Support," June 2005, and DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005.

Results

As of November 2005, the Office of the Assistant Secretary of Defense for Homeland Defense had improved many aspects of the Defense Critical Infrastructure Protection program. They published program policy, developed program standards, took steps to establish a Defense Field Agency, and improved controls for program funding. Much remains to be done as the program matures and continues to change in response to current events. The remaining paragraphs of this section document executed and planned actions and events organized to match our observations and recommendations.

Issue 1. Definitions

The Joint Staff J3, Deputy Director for Antiterrorism and Homeland Defense proposed changing the definition of *force protection* to include *all hazards*, in line with our recommendation. The Director, Defense CIP appropriately amended the definition of "mission assurance" and included it, along with other definitions, in DoD Directive 3020.40. As of November 2005, the definitions contained in DoD Directive 3020.40 were not included in Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms," (JP 1-02). Defense CIP officials agreed that the definitions should be included in JP 1-02 and that they would send the new definitions to the appropriate office in the Joint Staff.

Issue 2. Program Responsibilities

Prior to our review, program officials disagreed about primacy between the concepts of force protection and mission assurance. Antiterrorism program officials endorsed mission assurance as subordinate to force protection, while Defense CIP officials supported the opposite. ASD(HD) officials stated that our recommendation of equal importance under readiness generated positive discussion and was partially adopted. As of November 2005, Defense CIP program officials stated that they considered preparedness as the concept overarching mission assurance and force protection. However, representatives from the Joint Staff considered mission assurance an end state to be achieved through force protection, continuity of operations, and critical infrastructure protection. The lack of agreement demonstrates a need for additional work to unify the theory behind the programs.

Responsibility for programs, including Defense CIP, Information Assurance, Antiterrorism, Physical Security, and others, remained spread across multiple offices in the Office of the Secretary of Defense. Another remaining concern was the lack of an individual with assigned responsibility for the overall mission assurance and force protection constructs. However, acceptance of mission assurance as a complementary concept to force protection was increasing. Mission assurance was defined in DoD Directive 3020.40, stated as 1 of 12 objectives of the Strategy for Homeland Defense and Civil Support, and included as an action item in the Acting Deputy Secretary of Defense memorandum, "Implementation of the Strategy for Homeland Defense and Civil Support," dated June 24, 2005.

Based on the stated mission of the ASD(HD), we recommended a geographic division of program responsibilities. The Director, Defense CIP believed that program responsibilities were better allocated by function than by geography due to the seamless nature of networks and the idea that capabilities should not be bounded by geography. According to ASD(HD) officials, the limitations on military responses to Hurricane Katrina coupled with the military's response to the earthquake disaster in Karachi, Pakistan have raised questions about expanding the DoD's civil support role. These missions imply changing responsibilities for the ASD(HD) and renders our recommendation as stated inapplicable. As of November 2005, DoD Directive 5111.13, "Assistant Secretary of Defense for Homeland Defense," was not published. However, senior officials continued to realign program responsibilities within the Office of the Under Secretary of Defense for Policy, attempting to reduce gaps and overlaps. The Under Secretary of Defense for Policy should clearly divide responsibilities between the ASD(HD) and the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict in their charter directives.

Issue 3. Assessment Standards

All parties interviewed acknowledged the need for consistent standards. Defense CIP officials explained that they used the results of two initiatives to refine proposed standards. Representatives from the program office conducted a series of six pilot assessments in conjunction with Joint Staff Integrated Vulnerability Assessments (JSIVAs) performed by the Defense Threat Reduction Agency. They also worked with the Joint Staff to create a Defense CIP module used by assessors. Defense CIP program officials concluded from the second effort that the mission assurance and all-hazards focus of Defense CIP will likely preclude full integration into the force protection and antiterrorism JSIVA. In addition, the JSIVA remained focused on active duty warfighting assets. These conclusions reinforce our recommendations.

Defense CIP program officials stated they anticipated signature of interim guidance by the ASD(HD) in December 2005, with publication of a DoD Instruction within 180 days. The interim guidance document combined basic threat, vulnerability, and criticality standards into one document, applicable to all assets critical to DoD missions. Representatives from both the Joint Staff and DCMA stressed the importance of finalized standards for continued program progress.

Our review identified a lack of program emphasis on DoD nonwarfighting, National Guard, and non-DoD assets deemed critical to DoD missions. The National Guard

conducted JSIVAs of Guard-owned assets by using the Defense CIP module, and according to the Defense CIP Deputy Director for Operations, was prepared to incorporate new Defense CIP standards. The Defense Contract Management Agency, as the sector lead for the Defense Industrial Base, had several ongoing initiatives. It developed and used three Defense CIP related models: criticality determination, asset prioritization, and the risk of industrial failure. DCMA also drafted a Memorandum of Agreement to conduct Defense CIP assessments of non-DoD critical assets in the United States. As part of the non-DoD asset assessment effort, ASD(HD) worked with the National Guard to complete interstate compacts allowing trained teams to perform work outside of their home States. All responsible parties demonstrated significant progress, but non-DoD critical assets located outside the United States remained an issue.

Issue 4. Program Roles

The Principal Deputy Under Secretary of Defense for Policy approved the establishment of a field activity that will combine program management for Continuity of Operations, Continuity of Government, and Defense CIP. ASD(HD) planned to provide the field activity with authorization for 90 full-time equivalents: 60 for Continuity of Operations and Continuity of Government, and 30 for Defense CIP. It planned to staff the authorizations through transfer of 60 spaces from the Defense Logistics Agency and 30 spaces from the Defense Program Office for Mission Assurance. The field activity will count against the Washington Headquarters Services staffing allotment. The ASD(HD) Comptroller verified that he was programming for the field activity. This action is a good first step toward consolidating scattered mission assurance and force protection program efforts.

Issue 5. Program Funding

ASD(HD) actively pursued program implementation funding and established controls for its use. Defense CIP program funding for FYs 2004 through 2007 was allocated from the Office of the Comptroller to the ASD(HD) within the Program Operating Memorandum in a discrete program element. ASD(HD) planned to directly control and suballocate program budget authority for FYs 2006 and 2007. For FY 2006, the ASD(HD) Comptroller provided the Joint Staff, Defense sectors, and their own staff element with budget targets, and established a prioritized unfunded requirements list based on submissions. As of November 2005, they were prepared to write the program statement of work following congressional approval of the authorization bill.

ASD(HD) planned to decentralize Defense CIP execution to the Services while retaining advocacy of the Defense CIP program element. ASD(HD) stated that starting with the FY 2008 budget, it would require Service Program Element Managers to ensure funds are budgeted and executed to satisfy Defense CIP requirements outlined in DoD Directive 3020.40. ASD(HD) planned to distribute approximately 60 percent of the Defense CIP funding to combatant commands and Services and maintain control of 30 to 40 percent for running the field activity and 10 percent for new initiatives. ASD(HD) understood its responsibility for ensuring the Services adequately fund the program element.

Defense CIP stakeholders within DoD provided input and were kept informed of fiscal decisions through the governance council. The primary charter of the council was to determine program funding priorities. The council comprised 10 individuals, as shown in Table 2. The Joint Staff J34 representative stated that he acted as an advocate for the combatant commands and Services.

Table 2. Defense CIP Governance Council

1	Director, Defense CIP - USD(P)
2	Principal Staff Assistant - USD(AT&L)
3	Principal Staff Assistant - USD(I)
4	Principal Staff Assistant - USD(C)/CFO
5	Principal Staff Assistant - USD(P&R)
6	JCS - J34
7	Mil Dep Representative - Army
8	Mil Dep Representative - Navy
9	Mil Dep Representative - Air Force
10	DCMA - DIB Defense Sector Rep

Mitigating identified vulnerabilities remained an installation or Service issue. ASD(HD) representatives planned to oversee the prioritization and tracking of Defense CIP requirements through Joint Monthly Reviews and Joint Quarterly Reviews. ASD(HD) officials decided not to establish a Defense CIP fund for mitigation similar to the antiterrorism program's Combating Terrorism Readiness Initiatives Fund. They concluded that consolidating mitigation funds outside the Services would result in the Services reallocating an equivalent amount away from mitigation during their budget process.

Appendix A – Methodology

Crystal Focus Process

Crystal Focus is an independent and objective inspection or evaluation of a key DoD-wide program or process. The Crystal Focus process provides a transparent yet focused evaluation of DoD issues. Normally, senior leadership requests these evaluations. We seek requestor input to develop objectives and to tailor product formats to best convey our findings. Crystal Focus products highlight the most significant issues and provide timely recommendations for senior leadership action. We conduct the reviews in accordance with criteria in the "Quality Standards for Inspections" published by the President's Council on Integrity and Efficiency in January 2005. The project team performs follow-up on all recommendations resulting from a Crystal Focus project, normally 12 and 18 months after the project is completed. Prior to publishing the report, the Crystal Focus team briefs the results, observations, and recommendations to senior officials of the DoD Office of the Inspector General (IG); DoD senior management; the requestor of the review, and appropriate program managers. We provide program managers with the opportunity for formal comment and include their verbatim comments in the final report.

Scope

We reviewed the Defense CIP program. Specifically, we evaluated policy, organization, roles and responsibilities, and funding from two broad perspectives: (1) the effectiveness of program policy and structure, and (2) the value and impact of vulnerability assessments on installations.

We reviewed program policy and organization of the program at ASD(HD), and the impacts of policy decisions with the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. We evaluated program roles, responsibilities, and funding in the Office of the ASD(HD), the Defense Program Office for Mission Assurance, the Joint Staff, the Defense Threat Reduction Agency, and the Defense Contract Management Agency. We also reviewed the program impact, funding, and structure at U.S. Northern Command, U.S. European Command, and U.S. Pacific Command.

We performed this evaluation from June 2004 through November 2005, in accordance with the standards established by the President's Council on Integrity and Efficiency in the publication "Quality Standards for Inspections," March 1993 and the subsequent January 2005 update.

Limitations

We limited our review in three significant aspects. First, the ASD(HD) defined Defense Critical Infrastructure as "DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide." We did not evaluate cyber security policies for electronic network attack; we limited our review to

the physical aspects of network protection. Second, we did not contact nongovernmental organizations and contractors that own Defense Industrial Base assets identified as critical, due to time and resource constraints. Finally, we limited our evaluation to the Office of the Secretary of Defense, the Joint Staff, Unified Commands, and Defense Agencies because of limited program maturity and undefined impact on installations at the time of the review.

Work Performed

We conducted the evaluation as an early implementation review, with the goal of identifying vulnerabilities and successes and providing recommendations for improvement to a developing program. We focused on policy development, program organization, and implementation at higher headquarters. From June 2004 through February 2005, the team performed the following steps.

- We reviewed public law and Executive and Defense Department policy, regulations, and directives governing the Defense CIP program.
- We reviewed relevant reviews, audits, evaluations, inspections, and studies from the past 5 years associated with the program. Sources used included the Government Accountability Office, the Defense Science Board, and the DoD Inspector General.
- We conducted interviews with senior OSD and program officials and visited the following organizations:

  Assistant Secretary of Defense for Homeland Defense
  - Defense Program Office for Mission Assurance
  - Critical Infrastructure Program Integration Staff

  Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
  The Joint Staff
  - Combating Terrorism Directorate (J34)
  - Strategy and Policy Directorate (J5)

  U.S. Northern Command
  U.S. Pacific Command
  U.S. European Command
  Defense Threat Reduction Agency
  Defense Contract Management Agency

- We analyzed current and draft DoD policy and guidance.
- We discussed our results with program management prior to briefing our conclusions to the ASD(HD) in February 2005. We subsequently provided a series of "Observations" documenting the details and logic supporting our conclusions.

In October and November 2005, we conducted a follow-on review to document program improvement and determine outcomes based on our recommendations. The results of this review are shown on pages 24 through 27.

Appendix B – Briefing to the Assistant Secretary of Defense for Homeland Defense

Evaluation of Defense Installation Vulnerability Assessments

Project D2004-DIP0E2-0157

Office of the Inspector General, Department of Defense

Inspections and Policy

Inspections & Evaluations Directorate

Brief to

Hon. Paul McHale

Assistant Secretary of Defense
for Homeland Defense

February 17, 2005

George Marquardt
www.dodig.osd.mil

CIP Related Policy Response to GWOT

GLOBAL WAR ON TERRORISM (GWOT)

Early events such as the Khobar Towers and USS Cole bombings generated minor changes to organization and doctrine. The attacks of Sep 2001 shifted the focus to the Homeland and caused significant changes.

NATIONAL

Oct 2001 – EO13231 "Critical Infrastructure in the Information Age"

Oct 2001 - PL 107-56 US Patriot Act (includes the Critical Infrastructure Protection Act, 42 USC 5195c)

Nov 2002 - PL 107-296 Homeland Security Act (established the Department of Homeland Security)

Feb 2003 - "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets"

Dec 2003 – HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection" (one of a series of 12 policy directives published between Oct 2001 – Aug 2004)

DEPARTMENT OF DEFENSE

Oct 2002 – Change to Unified Command Plan (established NORTHCOM)

Feb 2003 – Office of the Assistant Secretary of Defense for Homeland Defense established

Inspections & Evaluations
A Crystal Focus Review

Doctrinal Construct

NATIONAL

The goal of the program is NATIONAL PREPAREDNESS, where "all-hazards preparedness" is defined as the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from domestic terrorist attacks, major disasters, and other emergencies.

(Homeland Security Presidential Directive 8, "National Preparedness," December 17, 2003).

DEPARTMENT OF DEFENSE

The defense equivalent is READINESS, defined as the ability of US military forces to fight and meet the demands of the national military strategy. It is the synthesis of two distinct but interrelated levels:

UNIT READINESS is the ability to provide Combatant Commanders with units capable of delivering designed outputs to execute assigned missions.

JOINT READINESS is the Combatant Commanders' ability to integrate and synchronize forces to execute assigned missions.

(Definition from Joint Publication 1-02, "The DoD Dictionary of Military and Associated Terms," as of February 2005)

Inspections & Evaluations
A Crystal Focus Review

DoD Doctrinal Construct

UNIT READINESS is a commander's responsibility and a Service-centric mission. One of the activities that allow Services to ensure readiness is (Force) PROTECTION.

(Force) PROTECTION is action taken to prevent or mitigate hostile actions against DoD personnel, resources, facilities, and critical information. This does not include actions to defeat an enemy or protect against accidents, weather, or disease (JP 1-02).

As defined, PROTECTION is primarily a defensive activity, applicable only to DoD assets, and limited to human threats.

JOINT READINESS is primarily a joint mission. One of the activities that allow Combatant Commanders to ensure readiness is (Mission) ASSURANCE.

(Mission) ASSURANCE is a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan (DoDD 3020.ff draft).

As defined, ASSURANCE is an external activity, applicable to any resource potentially impacting planned missions, and encompassing all hazards.

Inspections & Evaluations
A Crystal Focus Review

DoD Organization

Program responsibilities associated with PROTECTION and ASSURANCE are spread across multiple Under, Deputy, and Assistant Secretaries.

AT	ASD(SO/LIC)	DoDD 2000.12
CBRNE	USD(AT&L)	DoDI 6055.x [1]
COOP/COG	USD(P)	DoDD 3020.26
CIP	ASD(HD)	DoDD 5160.54 [2]
IA	ASD(NII)	DoDD 8500.1
Installation Prep	ASD(SO/LIC)	DoDI 2000.18 [3]
Physical Security	USD(I)	DoDD 5200.8

[1] ATSD(NCB) has primary responsibility for CBN (DoDD 5134.8). Various Instructions in the 6055 series for Radiological and High Explosives.

[2] Draft DoDD 3020.ff developed by ASD(HD).

[3] DoDI 2000.18 established guidelines for CBRNE emergency response. However, this may be outside ASD(SO/LIC) charter responsibilities (DoDD 5111.10).

OBSERVATION: Because doctrine and organization changes necessitated by the GWOT are incomplete, DoD PROTECTION and ASSURANCE concepts are disjointed and associated programs are poorly coordinated, resulting in inefficient implementation and less than optimal funding.

Inspections & Evaluations
A Crystal Focus Review

Impact on CIP

The evolution of doctrine and the failure to update definitions and organizational responsibilities result in five points of programmatic stress for the Defense Critical Infrastructure Program:

Asset Location - CONUS / OCONUS

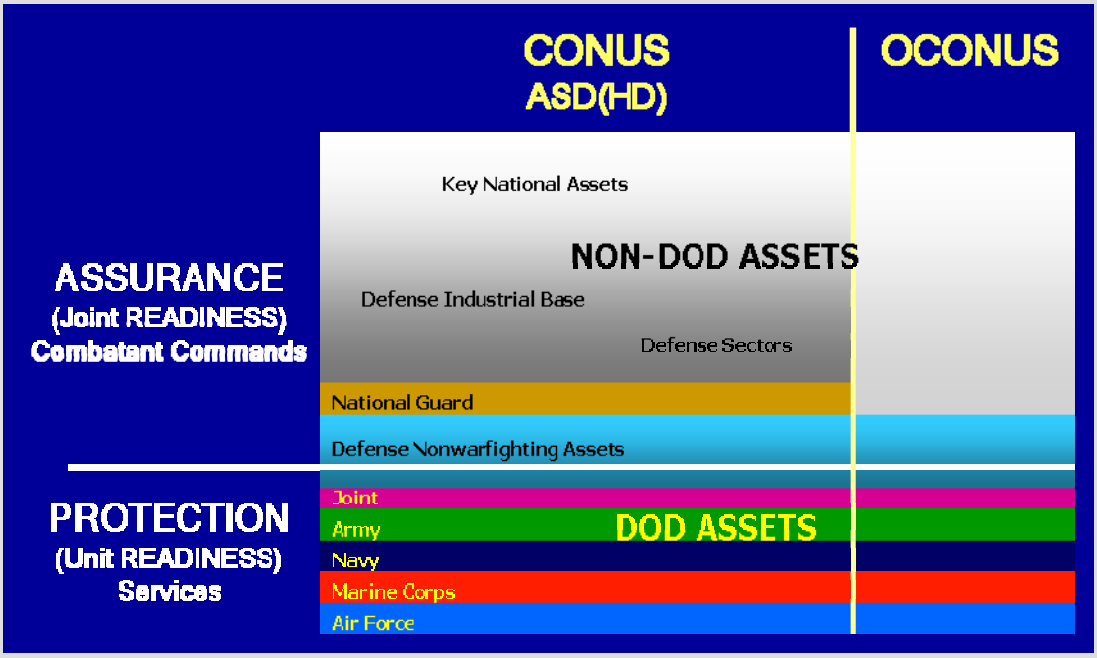
Asset Ownership - DoD / Non-DoD

Program Nexus – COCOMS / Service / Defense Sectors

Program Participation – Title 5 / Title 10 / Title 32

Threats Addressed - Terrorism / All-Hazard

DOD RESPONSIBILITIES BY LOCATION



2/17/2005 6

Inspections & Evaluations
A Crystal Focus Review

Desired Endstate

PROGRAM GOALS (DoDD 3020.ff - draft) :

Defense Critical Infrastructure is available as required.

The identification, prioritization, assessment, and assurance of Defense Critical Infrastructure is managed as a comprehensive program.

Vulnerabilities found in Defense Critical Infrastructure are remediated or mitigated based on risk.

DCIP will complement other DoD programs and efforts

MANAGEMENT ACTIONS: To effectively accomplish CIP program goals, management must ensure that:

1. Concepts are tightly defined and integrate with broader governing doctrine.
2. Program responsibilities are established in policy, and existing policy and authority is modified as necessary.
3. Priority for program efforts build on existing programs (fill in gaps) and minimize duplication of effort (overlaps).
4. Responsibilities are assigned within the program to reflect program focus and achieve program goals.
5. Stakeholders support or at a minimum acquiesce to the program philosophy and goals.
6. A mechanism is developed to ensure identified vulnerabilities receive sufficient consideration for funding.

Inspections & Evaluations
A Crystal Focus Review

Actions Taken

1. Concepts
   a. ensured program inclusion in ASD(HD) strategy and drafted program integrated risk management strategy.
   b. conducted serious efforts toward establishing common program definitions and strategic concepts.

2. Policy:
   a. worked toward publication of DoDD 5111.13.
   b. DoDD 3020.ff in final coordination at USD(P).
   c. pursued reorganization of USD(P) responsibilities.

3. Focus - recognized opportunity for and pursued systemic solutions, conducted a gap analysis, and remained sensitive to assessment impacts on commands.

4. Responsibilities:
   a. increased effectiveness of DoD CIP organization.
   b. developed methodology for Mission Area Analysis.
   c. recognized issues with DPO-MA responsibilities.

5. Stakeholders - included DoD players through routine coordination and expanded CIPIS, and recognized and assigned DIB responsibilities

6. Funding – pursued current year program funding, attempted to ensure stable funding over the POM.

Inspections & Evaluations
A Crystal Focus Review

Recommendations

1. Change definitions:
   a. delete "Force" from "Force Protection" and include "all-hazards" in JP 1-02.
   b. add "Assurance" to JP 1-02.
   c. change assessment eligible installations in DoDI 2000.16 to include DoD assets deemed "critical" by Combatant Commanders IAW CIP policy and standards.
   d. delete "overarching DoD framework" from "Mission Assurance" in DoDD 3020.ff and include elements from DoDD 5160.54 (Critical Asset Assurance Program, 1998).
2. Assign and modify program responsibilities:
   a. organize all PROTECTION and ASSURANCE activities under a "readiness" (preparedness) umbrella.
   b. increase efforts concerning non-DoD assets and adjust the Defense CIP program focus accordingly (requires a change to DoDD 3020.ff, para. 3.1 and 4.1).
   c. divide primacy for policy for PROTECTION and ASSURANCE programs geographically –
      1. CONUS and the approaches (suggest ASD(HD) – aligns with "charter" responsibilities).
      2. OCONUS (suggest ASD(SO/LIC) - requires modification of DoDD 5111.10).
   d. publish ASD(HD) charter (DoDD 5111.13).

Inspections & Evaluations
A Crystal Focus Review

Recommendations

3. Develop DCIP as a complementary program that fills gaps and minimizes duplication:

a. complete CIP assessment standards for non-DoD assets and unique CIP standards for DoD assets.

b. develop CIP assessments that review non-DoD assets and integrate with DTRA-JSIVA for DoD assets.

c. coordinate and fund "expert type" assessments for vital strategic DoD and non-DoD national assets.

4. Establish and modify responsibilities in the program:

a. develop desired outcomes and quantifiable metrics

b. develop and adopt standardized processes for determining criticality.

c. define the program roles that demonstrate DCIP is a Defense-wide program (broader than warfighting assets) –

1. Protection and Assurance Field Activity –

i. manage development and validation of training, assessment, and accreditation standards

ii. maintain common assessment databases, identify, prioritize, and track nonwarfighting assets

2. DTRA – conduct vulnerability assessments

3. Joint Staff - coordinate prioritization and funding between Combatant Commands and Services

4. Combatant Commands - determine criticality and track and prioritize identified mission-related vulnerabilities

Inspections & Evaluations
A Crystal Focus Review

Recommendations

d. establish policy that allows for adequate sharing and standard analysis and integration of threat information.

5. Continue to address all stakeholder concerns.

6. Establish CIP as a program in PPBE where ASD(HD):

a. develops organization and controls funding for dedicated program staff and support to stakeholders.

b. obtains funding for assessments.

c. advocates for mitigation funding from a centralized, prioritized database of risk-based vulnerabilities.

OVERARCHING RECOMMENDATION:

Separate CIP program and FSIVA development. Make FSIVA part of a larger coordination effort involving multiple OSD offices attempting to:

1. Incorporate and integrate all PROTECTION and ASSURANCE assessment standards including DCIP, JSIVA, IA, Physical Security, CBRNE, etc. into comprehensive modular FSIVA standards.

2. Conduct coordinated assessments through master scheduling including a common operating picture, modular FSIVA standards, and data sharing with all concerned parties to minimize the impact of multiple assessments on commands, installations, and critical non-DoD assets.

Inspections & Evaluations
A Crystal Focus Review

Acronym List

AT	Anti-Terrorism (Program)
CBRNE	Chemical, Biological, Radiological, Nuclear, and High Explosive (Weapons)
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
COOP	Continuity of Operations
COG	Continuity of Government
DTRA	Defense Threat Reduction Agency
DCIP	Defense Critical Infrastructure Program
DPO-MA	Defense Program Office – Mission Assurance
EO	Executive Order
FSIVA	Full Spectrum Integrated Vulnerability Assessment
GWOT	Global War on Terrorism
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
JSIVA	Joint Staff Integrated Vulnerability Assessment
PL	Public Law
Title 5	U.S. Code, Title 5, "Government Organization and Employees"
Title 10	U.S. Code, Title 10, "Armed Forces"
Title 32	U.S. Code, Title 32, "National Guard"

Appendix C – Management Comments

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, DC 20301-2600

HOMELAND
DEFENSE

DEC 2 3 2005

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

Subject: Defense Critical Infrastructure Program Evaluation

On January 16, 2004, the Assistant Secretary of Defense for Homeland Defense requested your assessment of the vulnerabilities to our critical defense infrastructure. After initial discussion, we agreed to expand the evaluation to address five broader policy and programmatic issues. On October 19, 2005, Colonel Forrest Sprester presented our staff with the results from that assessment.

Your staff identified five issues that highlight the opportunities and challenges our Defense Critical Infrastructure Program faces in its support to decision makers. The attached paper addresses your recommendations and provides a summary of actions we have undertaken with regard to your staff's recommendations.

I want to thank you for the outstanding work of your staff. Colonel Sprester and his team are to be commended for their professionalism, expertise, and dedication.

Peter F. Verga
Principal Deputy

Attachment:
As stated

CIP Directorate, OASD(HD)
Response to DoD IG Issues Related to
Evaluation of the Defense Critical Infrastructure Program (DCIP)

Issue 1: Definition Changes

Discussion:

- DoD(IG) states that the two terms used by DoD to define the primary activities associated with Critical Infrastructure Protection, "force protection" and "mission assurance," do not encompass all critical assets and potential threats.
- IG states that anti-terrorism policy should require assessments at activities that are deemed critical under CIP standards, regardless of the number of personnel impacted in order to help integrate activities an mitigate risk.

Recommendations:

1. Request the Director for Operational Plans and Joint Force Development, Joint Staff, amend the term "Force Protection" in JP 1-02 by deleting the word "Force" and including an "all hazards" component to ensure consistency with the intent of HSPD-8 [Homeland Security Presidential Directive #8].

   Disagree. Force protection is principally concerned with the physical protection of DoD personnel, equipment and facilities. While the definition states that force protection includes the protection of information, most in the information management community agree that information assurance is outside the AOR [Area of Responsibility] of the force protection community. Mission assurance is defined broadly enough to address all-hazards even though its focus is on assuring critical capabilities.

2. Amend the term "Mission Assurance" in draft DoDD 3020.ff by deleting the word "mission," and refine the definition to include specific policy considerations addressed in DoDD 5160.54.

   Disagree. DEPSECDEF's [Deputy Secretary of Defense] approval of DoDD 3020.40 establishes a definition for the term "mission assurance." DoDD 5160.54 is cancelled.

3. Request the Director for Operational Plans and Joint Force Development, Joint Staff include the revised "assurance" definition in JP 1-02.

   Agree.

4. ASD (SO/LIC) [Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict] should amend DoDI 2000.16, Para E3.1.1.26.7, "Antiterrorism Site Criteria," to allow Combatant Commanders to conduct vulnerability assessments of those DoD assets deemed critical under CIP standards.

   Agree.

   [Inspector General Note: We removed this recommendation from the final report.]

Issue 2: Program Responsibilities

Discussion:

- IG used HSPD-8, National Preparedness to develop recommendations and used the term "readiness". HSPD-8 uses "preparedness" in lieu of "readiness", defining it as "the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events."
- The IG uses the DoD JP 1-02 definition of "readiness", which is limited to military forces, and unit and joint readiness. This definition is different from the one used in the National Response Plan.
- IG asserts that CIP protection and assurance contribute to "readiness", but DCIP protection and assurance are not limited to military forces' ability to execute the National Military Strategy.
- IG cites the JP 1-02 definition for "protection" as derived from a narrower concept of force protection.
- The JP 1-02 definitions are insufficient and tailored to the originators' desired contexts desired.

Recommendations:

1. Organize Protection and Assurance programs and initiatives under a common overarching concept of all-hazards preparedness.

   Partially Agree. Agree that an overarching concept is needed to clarify responsibilities for protection and assurance policy and programs. However, "readiness," in the context of JP 1-02[1], is insufficient for DCIP and mission assurance because the definition is too narrowly circumscribed. In HSPD-7, "preparedness" includes military forces, public and private infrastructure as well as plans, procedures, policies, training, and equipment needed to prevent, respond to, and recover from major events. In this context, preparedness addresses interdependency or resiliency issues.

2. Complete DoDD 5111.13, amend DoDD 5111.10 to reflect geographic division of responsibility for protection and assurance policy and programs between HD [Homeland Defense] and SOLIC [Special Operations and Low Intensity Conflict].

   Disagree. HSPD-7, HSPD-8, and the DCIP require policy that acknowledges the importance of interdependencies between and among critical infrastructure assets. The President's directives imply that geographic and jurisdictional boundaries are irrelevant to critical infrastructures, like transportation, information or energy, which exist across such boundaries. The IG use of the term "readiness" with its narrow focus on military

[1] Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms." The ability of US military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels. a. unit readiness--The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. b. joint readiness--The combatant commander's ability to integrate and synchronize ready combat and support forces to execute his or her assigned missions. See also military capability; national military strategy.

forces and Joint/Unit readiness[2] is unsuitable for critical infrastructure policy and program responsibilities. Dividing OSD responsibilities within OSD by geography would decrease the effectiveness of critical infrastructure efforts.

Issue 3: Assessment Standards

Discussion:

- IG report states that "as of February 2005, the Defense Critical Infrastructure Program" did not provide sufficient "deployed capabilities". In addition, prioritization of efforts and application of program resources was not optimized to address non-war fighting critical assets.
- IG report states that the Full Spectrum Integrated Vulnerability Assessment (FSIVA) standards document has a number of deficiencies.
- IG report states, "Homeland Security Presidential Directive No. 7 explicitly assigns responsibility to the DoD for protection of the Defense Industrial Base (DIB)." However, HSPD-7 does not state that DoD is responsible for the protection of the DIB. HSPD-7 correctly assigns DoD responsibility for the DIB as the Sector Specific Agency to coordinate infrastructure protection activities for the DIB.

Recommendations:

1. Complete CIP assessment standards for non-DoD assets and unique CIP standards for DoD assets.

   Agree.

2. Develop CIP assessments that review non-DoD assets and integrate with Defense Threat Reduction Agency-Joint Staff Integrated Vulnerability Assessment (DTRA-JSIVA) for DoD assets.

   Partially Agree. DTRA-JSIVA assessments support force protection. The standards for JSIVAs are mature, but are limited to the physical security of people, facilities and equipment within the DoD installation perimeter. DCIP requires assessments to address physical, cyber, personnel and procedural considerations. DCIP requires non-DoD-owned critical asset assessments to determine the facility or institution economic viability, and to identify supply chain relationships.

3. Coordinate and fund "expert type" assessments for vital strategic DoD and non-DoD national assets.

   Agree.

4. Increase Critical Infrastructure Protection program activities to assure the availability of DoD non-war fighting, National Guard, and non-DoD assets critical to DoD missions.

   Agree.

Issue 4: Program Roles

Discussion:

[2] ibid

- The Report states that the "Defense Critical Infrastructure Protection (DCIP) program organization was inadequate to achieve desired homeland defense strategic objectives."
- The Report states that ASD(HD) responsibilities are limited to U.S. Territories and the approaches. DoDD 3020.40 now assigns the global DCIP mission to the ASD(HD). As such, the report conflicts with the global infrastructure protection responsibility of the Director, CIP. Furthermore, critical infrastructure addresses physical and cyber nodes and links in a supply chain of products and services that transcend geographic and jurisdictional boundaries.

Recommendations:

1. The Under Secretary of Defense for Policy should establish a field activity responsible for implementing and monitoring Department protection and assurance programs.

   Partially agree. ASD(HD) is considering a broader set of requirements for a Field Activity to support the overall HD mission, to include those for implementing and monitoring protection and assurance programs.

   Primary responsibilities for the Field Activity would include:

   a. The development, validation, and accreditation of assessment standards and training standards for assessors;

   Agree

   b. The standardization, consolidation, and storage of facility infrastructure and vulnerability assessment data;

   Agree

   c. The analysis of data and identification of protection and assurance issues with impact across non-war fighting assets or DoD wide applicability; and

   Agree

   d. The obtaining, integration, and sharing of relevant threat data with assessing organizations.

   Agree

2. The Assistant Secretary of Defense for Homeland Defense should publish policy that assigns responsibility for the:

   a. Conducting of Defense Critical Infrastructure program vulnerability assessments

   Agree

   b. Standardization of definitions and criteria used to determine asset criticality; and

   Agree

   c. Development of quantifiable program metrics.

   Agree

(Issue 5 was not addressed by the DoD IG.)

Issue 6: Funding DCIP in PPBE

Discussion:

- The Report states that "DCIP planning and programming was inadequate to reduce critical vulnerabilities." The DCIP concept is that asset owners/operators are responsible for resourcing and making changes, to the assets for which they are responsible, to include vulnerability mitigation and remediation. The DCIP provides asset owners with justification for funding requirements submitted to the PPBE system. Asset owners/operators determine which actions are most appropriate to address vulnerabilities.
- The Report states that a significant concern is how DCIP programs, at the command level, lack established policy addressing program and mitigation funding. DoDD 3020.40 provides overall program direction and guidance. Asset owners/operators are responsible for mitigation and remediation funding.
- The Report states that programmatic inclusion in the PPBE system was necessary to develop the program. In addition, DoD components must submit funding requests to the PPBE system.
- The Report states that lack of stable funding was detrimental to long term assessment planning. Additionally, installation commanders were frustrated by the insufficient resources used to mitigate vulnerabilities. Consistent with DoDD 3020.40, DoD components must resource their DCIP activities including component vulnerability assessments for identified critical assets.
- The Report states that decentralized funding and a lack of centralized priorities or oversight discourage mitigation efforts. The Director, CIP is implementing a process to prioritize assessments of DoD strategic critical assets. DoD components may fund and prioritize DCIP activities within their respective areas of responsibility, consistent with the Secretary's direction and guidance.

Recommendations:

1. Establish the Critical Infrastructure Protection program in the PPBE system and control and coordinate program implementation funding.

   Agree.

2. Advocate for mitigation funding and a consolidated, prioritized database of risk-based vulnerabilities identified through a coordinated assessment process.

   Agree.

Appendix D – Acronym List

ASD(HD)	Assistant Secretary of Defense for Homeland Defense
AT	Antiterrorism (Program)
CIP	Critical Infrastructure Protection
CONUS	Continental United States (48 Contiguous States)
DTRA	Defense Threat Reduction Agency
DCIP	Defense Critical Infrastructure Program
DPO-MA	Defense Program Office for Mission Assurance
IG	Inspector General
JP	Joint Publication
JSIVA	Joint Staff Integrated Vulnerability Assessment
OCONUS	Outside the Continental United States
OSD	Office of the Secretary of Defense
PPBE	Planning, Programming, Budgeting, Execution
PDD	Presidential Decision Directive
Y2K	Year 2000

This Page Intentionally Left Blank

Appendix E – Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Policy
    Assistant Secretary of Defense for Homeland Defense
    Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

Department of the Army

Inspector General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Inspector General, Department of the Air Force

Joint Staff and Unified Commands

Director of the Joint Staff

Other Defense Organizations

Defense Contract Management Agency
Defense Threat Reduction Agency

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform

THE MISSION OF THE OIG DoD

The Office of Inspector General of the Department of Defense was established by Congress as one of the "independent and objective units [within listed 'establishments,' including the Department of Defense] to conduct and supervise audits and investigations relating to the programs and operations of those establishments." As the principal advisor to the Secretary of Defense in all Inspector General matters, the Inspector General serves as an extension of "the eyes, ears, and conscience" of the Secretary. In support of the mission of the Department of Defense, the Office of the Inspector General endeavors to:

- "Provide leadership…to promote economy, efficiency and effectiveness;"
- Prevent and detect "fraud, waste, and abuse;"
- "Provide policy direction for audits and investigations;"
- "Provide a means for keeping the [Secretary of Defense] and the Congress fully and currently informed about problems and deficiencies;" and
- "Give particular regard to the activities of the internal audit, inspection, and investigative units of the military departments with a view toward avoiding duplication and insuring effective coordination and cooperation."

TEAM MEMBERS

The Homeland Defense Division, Inspections and Evaluations Directorate, Office of the Deputy Inspector General for Inspections and Policy, Office of Inspector General for the Department of Defense prepared this report. Personnel who contributed to the report were Col Forrest R. Sprester, Division Chief; Mr. George P. Marquardt, Team Leader; Mr. Joe A. Baker; Lt Col Michael T. Luft; Lt Col John N. Camperlengo; Lt Col Heidie R. Rothschild; and Maj Chad W. Lusher.

ADDITIONAL REPORT COPIES

Contact us by phone, fax, or e-mail:

Inspections and Evaluations Directorate, Deputy Inspector General for Inspections and Policy
COM: 703.604.8772 (DSN 664.8772)
FAX: 703.604.9769
E-MAIL: crystalfocus@dodig.mil

Murrah Building, Oklahoma City
April 26, 1995

Domestic Terrorism
- US Government Facility

Photograph Courtesy of the City of Oklahoma City

Khobar Towers, Saudi Arabia
June 25, 1996

International Terrorism
- Foreign Facility

Photograph Courtesy of Department of Defense

USS Cole, Yemen
October 12, 2000

International Terrorism
- US Asset

Photograph Courtesy of United States Navy

World Trade Center, New York
September 11, 2001

International Terrorism
- US Business Facility

Photograph by SSGT Michelle Leonard,
Courtesy of United States Air Force

New Orleans
August 29, 2005

Natural Event
- US Infrastructure

Photograph by Jocelyn Augustino,
Courtesy of the Federal Emergency
Management Agency.

A great people has been moved to defend a great nation. Terrorist attacks can shake the foundations of our biggest buildings, but they cannot touch the foundation of America. These acts shattered steel, but they cannot dent the steel of American resolve.

Statement by the President in His Address to the Nation
September 11, 2001