

Executive Summary

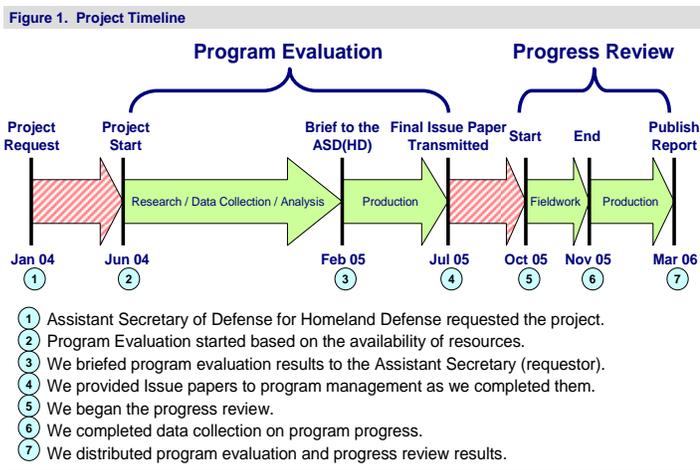
Defense Installation Vulnerability Assessments

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.



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:

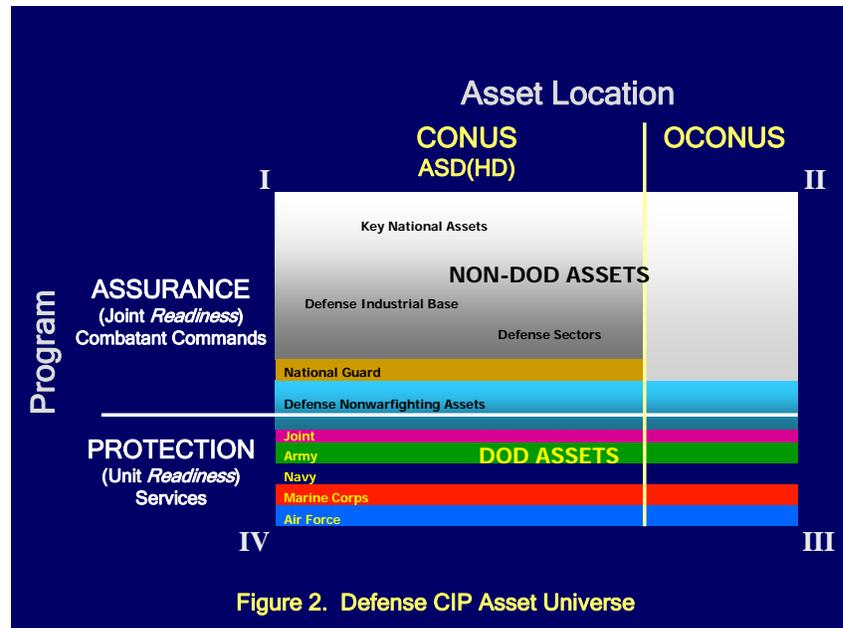
- published program strategy, prepared draft policy, and conducted program assessments and gap analyses;
- increased staffing, reorganized responsibilities, and actively engaged stakeholders on multiple levels;
- proposed strategic concepts, developed common program definitions, and pursued systemic 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 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.