



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 2, 2008

The Honorable Solomon P. Ortiz
Chairman
The Honorable J. Randy Forbes
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

The Honorable William T. Akin
House of Representatives

Subject: *Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*

The Department of Defense (DOD) relies on a global network of critical physical and cyber infrastructure to project, support, and sustain its forces and operations worldwide. The incapacitation, exploitation, or destruction of one or more of its assets would seriously damage DOD's ability to carry out its core missions. To identify and help assure the availability of this mission-critical infrastructure, in August 2005, DOD established the Defense Critical Infrastructure Program (DCIP), assigning overall responsibility for the program to the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]).¹

Since 2006, ASD(HD&ASA) has collaborated with the Joint Staff to compile a list of all DOD- and non-DOD-owned infrastructure essential to accomplish the *National Defense Strategy*.² Each critical asset on the list must undergo a vulnerability assessment, which identifies weaknesses in relation to potential threats and suggests options to address those weaknesses.

¹ Earlier programs analogous to DCIP can be traced back to 1998. ASD(HD&ASA) has been responsible for developing and ensuring implementation of critical infrastructure protection policy and program guidance since September 2003.

² Department of Defense, *The National Defense Strategy of the United States of America* (Washington, D.C.: March 2005). *The National Defense Strategy* outlines DOD's approach to the defense of the nation and its interests, establishing four strategic objectives: (1) secure the United States from direct attack, (2) secure strategic access and retain global freedom of action, (3) strengthen alliances and partnerships, and (4) establish favorable security conditions.

Report Documentation Page

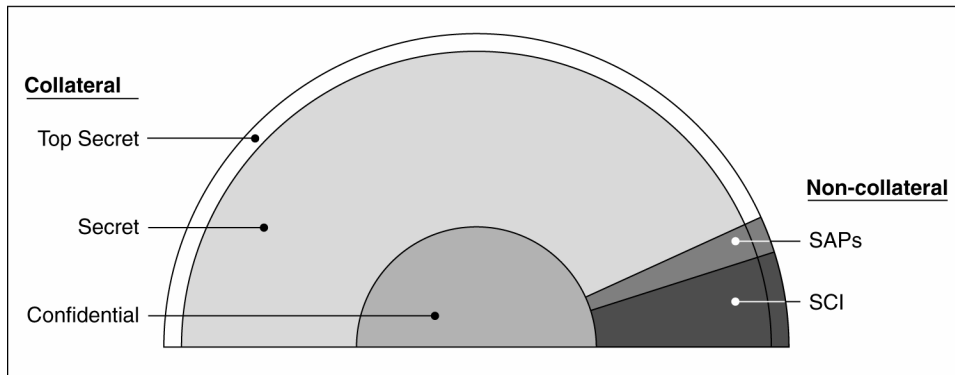
Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 02 APR 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Data and material designated as Sensitive Compartmented Information (SCI)³ or associated with Special Access Programs (SAP)⁴ are among the nation’s most valued and closely guarded assets, and DOD faces inherent challenges in incorporating them into DCIP. The number of individuals authorized to access SCI and SAPs is a relatively small subset of those authorized to access collateral-level classified information—that is, Confidential, Secret, or Top Secret information. The relationship between collateral, SCI, and SAP designations is depicted in figure 1.

Figure 1: Relationship between Collateral, SCI, and SAP Designations



Source: GAO analysis.

Note: The areas shown here represent categories of national security information. All classified information is Confidential, Secret, or Top Secret. Information classified at these levels but not subject to any additional safeguarding and access requirements is collateral information. Some information that is classified Secret or Top Secret also falls under an SCI or SAP designation; that information then becomes non-collateral. The relative size of each area is illustrative only.

You requested that we review a number of issues related to defense critical infrastructure. To date, we have issued two reports in response to that request. Our first report⁵ examined the extent to which DOD had developed a comprehensive management plan for DCIP and had identified, prioritized, and assessed defense critical infrastructure. Our second report⁶ examined DOD’s efforts to implement a risk management approach for critical assets in the Defense Industrial Base Defense Sector. As agreed with your offices, we plan to issue reports later this year that

³ SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.

⁴ Executive Order 12958 states that a SAP shall be established only when the program is required by statute or upon a specific finding that the vulnerability of, or threat to, specific information is exceptional, and the normal criteria for determining eligibility for access to information classified at the same level is insufficient to protect the information from unauthorized disclosure. SAPs impose safeguarding and access requirements exceeding those normally required for collateral information at the same level of classification. Collateral-level information is information identified as national security information (Confidential, Secret, or Top Secret) but not subject to enhanced security protection required for SCI or SAP information.

⁵ GAO, *Defense Infrastructure: Actions Needed to Guide DOD’s Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure*, GAO-07-461 (Washington, D.C.: May 24, 2007).

⁶ GAO, *Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DOD’s Risk Management Approach for the Defense Industrial Base*, GAO-07-1077 (Washington, D.C.: Aug. 31, 2007).

examine actions DOD has taken to assure the availability of its critical infrastructure in the Transportation; Space; Intelligence, Surveillance, and Reconnaissance; Global Information Grid; and Public Works Defense Sectors.

As part of our ongoing work on DOD's critical infrastructure protection efforts, this report focuses on challenges DOD faces in incorporating critical SCI and SAP assets into DCIP. Specifically, this report evaluates the extent to which DOD is (1) identifying and prioritizing critical SCI and SAP assets in DCIP and (2) assessing critical SCI and SAP assets for vulnerabilities in a comprehensive manner consistent with that used by DCIP for collateral-level assets.

To determine the extent to which DOD is identifying and prioritizing critical SCI and SAP assets in DCIP and assessing them for vulnerabilities using DCIP criteria, we reviewed guidance, critical asset lists, planning documents, and other relevant documentation, and we interviewed officials from the following DOD organizations: the Office of the ASD(HD&ASA), the Joint Staff Deputy Directorate for Antiterrorism and Homeland Defense, the Office of the Under Secretary of Defense for Intelligence, the DOD Special Access Program Central Office, the Defense Intelligence Agency, the Defense Contract Management Agency, and the nine geographic and functional combatant commands.⁷ We conducted this performance audit from September 2007 through February 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Although DOD Directive 3020.40 calls for the identification and prioritization of all defense critical infrastructure, DOD has not taken adequate steps to ensure that highly sensitive critical assets associated with SCI and SAPs are accounted for, either through DCIP or a comparable process. The Joint Staff has tasked DOD organizations to submit lists of critical assets classified at the collateral level only—in part, to facilitate vetting and sharing critical asset lists across the department. As a consequence, some DOD organizations have omitted SCI and SAP assets from their submissions. For example, the Defense Intelligence Agency—the DOD lead agent for the Intelligence, Surveillance, and Reconnaissance Defense Sector—has not forwarded to the Joint Staff a list of over 80 assets it has identified as critical, because neither the Joint Staff nor ASD(HD&ASA) has fully incorporated provisions for including SCI data into DCIP. Although ASD(HD&ASA) and Joint Staff officials have

⁷ The geographic combatant commands are the U.S. Central Command, U.S. European Command, U.S. Northern Command, U.S. Pacific Command, and U.S. Southern Command. (A sixth geographic combatant command, the U.S. Africa Command, remains subordinate to the European Command and, therefore, was not examined separately for this report.) The functional combatant commands are the U.S. Joint Forces Command, U.S. Special Operations Command, U.S. Strategic Command, and U.S. Transportation Command.

initiated some actions to increase their access to SCI—for example, by requesting additional SCI clearances for staff and pursuing means to store and share SCI data—these actions are not likely to resolve information-sharing problems across the department because many officials in other DCIP organizations may still lack access to SCI. Additionally, DOD officials told us that stringent “need to know” requirements for SAP information will likely prevent ASD(HD&ASA) and other DCIP officials from obtaining greater access to information on SAP assets in the foreseeable future. By excluding SCI and SAP infrastructure, DOD’s processes for soliciting critical asset information do not result in consistent and comprehensive identification and prioritization of all critical infrastructure. Yet ASD(HD&ASA) has not pursued alternative approaches, such as partnering with other DOD organizations that have greater SCI and SAP access, to develop parallel identification and prioritization processes. Unless critical SCI and SAP assets are identified and prioritized, DOD will lack sufficient information to assure the availability of the department’s most critical assets.

DOD guidance requires all critical infrastructure to be assessed for vulnerabilities using DCIP standards and benchmarks, but because SCI and SAP assets have not been reported as critical, they do not receive these assessments. Should any unreported critical SCI assets be reported under DCIP, the Defense Threat Reduction Agency has personnel who possess SCI clearances, and therefore could assess those assets. However, because of the greater access restrictions placed on SAP data, Defense Threat Reduction Agency officials are unlikely to gain access to the highly sensitive information needed to assess SAP assets. Separately from DCIP, the Defense Intelligence Agency assesses the vulnerabilities of SCI and SAP assets. However, those assessments are intended to support information and physical security rather than mission assurance. Accordingly, they do not include certain key elements of the assessments administered under DCIP, such as a mission-based orientation and an all-hazards analysis. The guidance the Defense Intelligence Agency uses to assess SCI and SAP assets focuses on the need to secure information from unauthorized disclosure rather than on the need to maintain continuity of mission-essential functions, and it emphasizes human threats, such as terrorism, rather than all potential hazards. Because of these fundamental differences, the Defense Intelligence Agency’s assessments of SCI and SAP assets cannot substitute for the mission-based, all-hazards vulnerability assessments required by DCIP. As a result, DOD lacks a consistent process for assessing its collateral and its more sensitive critical assets. Without using a consistent vulnerability assessment process for all its critical assets, including SCI and SAP assets, DOD cannot effectively analyze the comparative value of risk reduction actions.

We are recommending that ASD(HD&ASA) develop a process to identify, prioritize, and assess critical SCI and SAP assets in a manner consistent with DCIP, and amend its DCIP security classification guidance to specifically address how SCI and SAP critical infrastructure information should be treated.

In written comments on a draft of this report, DOD generally agreed with our recommendations. DOD’s comments are discussed in more detail at the end of this

report and are reproduced in full in enclosure I. DOD also provided us with technical comments, which have been incorporated where appropriate.

Background

Recognizing that it is neither practical nor feasible to protect its entire infrastructure against every possible threat, DOD is pursuing a risk management approach to help direct limited resources to higher-priority, higher-risk assets. DOD's risk management approach is based on assessing criticality, threat, vulnerability, and the ability to respond to incidents. Criticality assessments evaluate and prioritize assets on the basis of their importance to mission success. Threat assessments identify and evaluate potential threats to critical assets before they materialize, on the basis of capabilities, intentions, and past events. Vulnerability assessments analyze weaknesses in relation to identified threats and suggest options to address those weaknesses. DOD's risk management approach also includes an assessment of the ability to respond to, and recover from, an incident.

In response to the guidance contained in *Homeland Security Presidential Directive 7*,⁸ DOD formalized its critical infrastructure efforts on August 19, 2005, by issuing DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)*, which established the program and assigned overall responsibility to ASD(HD&ASA). DOD Directive 3020.40 requires, among other things, that ASD(HD&ASA) develop and ensure implementation of DCIP policy and program guidance for the identification, prioritization, and protection of defense critical infrastructure.

Pursuant to DOD Directive 3020.40, DOD has defined 10 virtual, functionally-based defense sectors comprising the critical infrastructure that crosses traditional organizational boundaries, and it has appointed a lead agent for each sector. The 10 defense sectors and their corresponding lead agents are listed in table 1.

⁸ *Homeland Security Presidential Directive 7*, issued in December 2003, requires, among other things, that all federal departments and agencies identify, prioritize, and coordinate the protection of critical infrastructure and key resources from terrorist attacks. DCIP encompasses the full spectrum of threats—ranging from terrorist attacks to natural disasters and catastrophic accidents—that can adversely affect critical defense infrastructure.

Table 1: Defense Infrastructure Sectors and Corresponding Lead Agents

Defense infrastructure sector	Defense infrastructure sector lead agent
Defense Industrial Base	Defense Contract Management Agency
Financial Services	Defense Finance and Accounting Service
Global Information Grid	Defense Information Systems Agency
Health Affairs	Assistant Secretary of Defense for Health Affairs
Intelligence, Surveillance, and Reconnaissance	Defense Intelligence Agency
Logistics	Defense Logistics Agency
Personnel	Under Secretary of Defense for Personnel and Readiness
Public Works	U.S. Army Corps of Engineers
Space	U.S. Strategic Command
Transportation	U.S. Transportation Command

Source: GAO analysis of DOD data.

ASD(HD&ASA) and the Joint Staff have tasked the combatant commands, military services, field activities, defense agencies, and defense infrastructure sector lead agents with nominating infrastructure necessary to accomplish the goals specified in the *National Defense Strategy*. The combatant commands, in collaboration with the Joint Staff, identify and prioritize DOD missions that are the basis for determining infrastructure criticality. The military services, as the principal owners of DOD infrastructure, identify and link infrastructure to specific combatant command mission requirements. Defense infrastructure sector lead agents address the interdependencies among infrastructure that cross organizational boundaries, and evaluate the cascading effects of degraded or lost infrastructure on other infrastructure assets. Assets nominated by the combatant commands and services have been assembled into a consolidated draft critical asset list, which ASD(HD&ASA) will use as the basis for a final list. The Joint Staff plans to send the latest iteration of the draft list to ASD(HD&ASA) in April 2008. ASD(HD&ASA) officials told us they expect to approve and issue a final critical asset list within 90 days of receiving a final draft list from the Joint Staff, which will include assets nominated by the defense infrastructure sector lead agents.

According to DCIP guidance,⁹ all defense critical assets must undergo vulnerability assessments. These assessments, performed primarily by the Defense Threat Reduction Agency or by asset owners themselves, follow a set of standards and benchmarks developed and maintained by ASD(HD&ASA).¹⁰ DCIP assessments use a mission-assurance approach; that is, they discern what weaknesses, if any, threaten an asset's continued availability to support its associated defense missions. This

⁹ Draft DOD Instruction 3020.n Defense Critical Infrastructure Program (DCIP) Management, undated.

¹⁰ In addition to the Defense Threat Reduction Agency and asset owners, the Defense Contract Management Agency and the National Guard also conduct DCIP assessments on defense industrial base assets using the same methodology.

mission-based analysis, according to DCIP standards and benchmarks,¹¹ requires assessment teams to consider an exhaustive set of potential hazards, including chemical, biological, radiological, nuclear, and explosive events; electromagnetic pulse; sabotage; projectile impact; cyber threats; arson; earthquakes, hurricanes, fire, and other natural disasters or weather events; collocated construction or digging activities; work stoppage or strike; and wildlife activity. DCIP's mission-assurance, all-hazards approach mirrors risk management strategies developed by the Department of Homeland Security, with the intention of providing a sound and systematic basis for deciding whether and how to accept, reduce, or offset risk to DOD's most mission-critical infrastructure.

DOD Has Not Included SCI and SAP Assets in Its Identification and Prioritization of Critical Infrastructure

Although DOD Directive 3020.40 calls for the identification and prioritization of all defense critical infrastructure and the development of policies that promote information sharing while properly safeguarding sensitive data, DOD has not taken adequate steps to account for critical infrastructure associated with SCI and SAPs, either through DCIP or an alternative approach. DOD organizations have submitted critical assets at the collateral level only, because the instructions they received did not address SCI or SAP assets. Moreover, key ASD(HD&ASA) officials involved with DCIP are not authorized to access SCI and SAP data, even if such data were submitted to them.

DOD Organizations Have Not Reported SCI and SAP Critical Assets

The Joint Staff, in preparing the critical asset list on behalf of ASD(HD&ASA), gave written instructions to DOD organizations on how to submit critical assets at the Secret or Top Secret levels; however, these instructions did not address how to submit critical SCI or SAP assets. The *DCIP Security Classification Guide*¹²—which describes what information related to critical infrastructure meets the standards of Confidential, Secret, or Top Secret at the collateral level—also does not specifically address SCI or SAP data related to critical infrastructure. The Joint Staff instructions and the guide do not rule out the designation of some critical asset information as SCI or SAP, but officials from two DOD organizations told us that the lack of explicit guidance on how to treat SCI and SAP data caused them not to fully report their critical assets. The Defense Intelligence Agency, the lead agent for the Intelligence, Surveillance, and Reconnaissance Defense Sector, has compiled a list of over 80 assets nominated by both the Defense Intelligence Agency and by the National Security Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, the military service intelligence activities, and the combatant command intelligence staffs. Defense Intelligence Agency officials told us that they have not forwarded the list to the Joint Staff because provisions for including SCI

¹¹ ASD(HD&ASA), *Defense Critical Infrastructure Program Assessment Standards and Benchmarks* (May 30, 2006).

¹² ASD(HD&ASA), *Defense Critical Infrastructure Program (DCIP) Security Classification Guide* (May 15, 2007) (For Official Use Only).

data have not been fully incorporated into DCIP. Similarly, officials at the Defense Contract Management Agency, the lead agent for the Defense Industrial Base Defense Sector, told us they have not reported any critical assets associated with SAPs because they believe that DCIP policies do not require them to do so. DCIP policies make no such exception for SAP infrastructure, but the lack of explicit guidance concerning SCI and SAPs has led DOD organizations not to report some SCI and SAP assets as critical.

In further explaining why the DOD critical asset list has been kept at the collateral level, Joint Staff and ASD(HD&ASA) officials stated that highly classified information would be difficult to share among all relevant DCIP stakeholders because of the limited number of individuals who have access to SCI and SAPs. The stringent access controls on SCI and SAP information would significantly restrict ASD(HD&ASA)'s ability to distribute among DCIP organizations any critical asset list that includes SCI or SAP infrastructure. Nevertheless, until DOD develops the means to identify and prioritize critical SCI and SAP assets, it cannot assure the availability of all critical defense infrastructure in a consistent and comprehensive way.

During the course of our review, the Joint Staff issued new instructions to DOD organizations, requesting them to submit their lists of critical SCI assets. Joint Staff officials told us that they have had discussions with the Defense Intelligence Agency about obtaining its SCI-level list of critical intelligence, surveillance, and reconnaissance infrastructure. These actions represent important initial steps toward identifying and prioritizing critical SCI infrastructure; however, they remain in their initial phases only. Joint Staff officials acknowledged that DOD has not taken similar actions to begin accounting for SAP infrastructure.

Key ASD(HD&ASA) Officials Are Not Authorized to Access SCI or SAP Data

A related barrier to including SCI and SAP assets in the DOD critical asset list is DCIP officials' lack of authority to access information pertaining to these highly sensitive programs. At the time of our review, key ASD(HD&ASA) personnel involved with DCIP were not authorized to handle SCI data. Similarly, ASD(HD&ASA) personnel had not been granted access to any SAPs, and did not expect to gain access in the foreseeable future. DOD policy¹³ imposes a stringent standard for meeting the "need to know" criterion: to handle SAP information an individual must "materially and directly contribute" to the individual SAP to which he or she requests access. DOD officials responsible for setting departmental SAP policy told us that ASD(HD&ASA) staff would almost certainly not qualify to access SAP information for the purpose of identifying and prioritizing defense critical infrastructure. For the same reason, according to an Air Force headquarters official responsible for SAPs, defense industrial base firms involved in SAPs would be reluctant to discuss their potential

¹³ DOD, *Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement* (April 1, 2004). Executive Order 12958, as amended, calls for agency heads to establish and maintain systems of accounting for the SAPs created under their authority.

critical assets with the Defense Contract Management Agency or other DCIP officials.¹⁴

ASD(HD&ASA) officials are aware of these issues and have taken some steps to resolve them. They have requested SCI clearances for additional personnel, have identified a computer terminal belonging to another DOD organization that could be used to transmit and receive SCI data, and have requested a computer authorized to store and process SCI data. Once ASD(HD&ASA) is able to handle and store SCI data, it will have access to the Intelligence, Surveillance, and Reconnaissance Defense Sector's critical asset list.

However, ASD(HD&ASA) has not taken similar actions to address its lack of access to SAPs. At the time of our review, ASD(HD&ASA) officials had limited coordination with DOD's SAP Central Office, the primary point-of-contact on all issues involving defense SAPs, and limited coordination with other defense organizations to discern what amount of critical infrastructure might reside in those programs. DOD officials responsible for SAP policy told us that most defense SAPs involve acquisition programs. The Defense Contract Management Agency, which is tasked with analyzing acquisition infrastructure, has compiled a sector-specific list of critical assets, but its list contains no SAP infrastructure. Defense Contract Management Agency officials acknowledged the need to identify critical SAP assets, but told us they had no plan for doing so.

Moreover, actions taken by ASD(HD&ASA) officials to increase their own SCI and SAP access will not be sufficient to address information-sharing problems across other DOD organizations with key roles in DCIP. For example, draft DCIP guidance¹⁵ calls for the military services, combatant commands, field activities, defense agencies, defense infrastructure sector lead agents, and other DOD organizations to review and validate the draft critical asset list once it has been compiled. But DOD officials told us that many DCIP personnel at these organizations are unlikely to be granted SCI or SAP access, denying them the authorization required to validate any critical asset list that includes SCI or SAP infrastructure.

Although DOD Directive 3020.40 tasks ASD(HD&ASA) with developing policies to promote information sharing while safeguarding sensitive data from disclosure, it has not pursued potential means of balancing these competing needs in the case of SCI and SAP infrastructure. For example, ASD(HD&ASA) has not explored the option of partnering with the Defense Intelligence Agency or the SAP Central Office to develop parallel identification and prioritization processes. These two organizations, or other DOD entities with the necessary access, could compile and maintain separate critical asset lists for SCI and SAP infrastructure, using standards consistent with those currently applied to collateral assets under DCIP. Such an approach could potentially fulfill DOD requirements for comprehensive risk management while respecting the extraordinary sensitivity of SCI and SAP data; to date, however, DOD has not taken

¹⁴ GAO-07-1077.

¹⁵ ASD(HD&ASA), *Critical Asset Identification Process* (draft) (September 1, 2007).

steps to pursue either this or similar options. Unless DOD revises or supplements its identification and prioritization process to resolve information-sharing problems, the omission of SCI and SAP assets will continue to limit DOD's awareness of its critical infrastructure.

SCI and SAP Vulnerability Assessments Are Not Consistent with Those Performed on Collateral-Level Assets

Although DOD guidance requires that all critical infrastructure be assessed for vulnerabilities using DCIP standards and benchmarks, SCI and SAP assets have not received DCIP assessments because they have not been reported as critical. The Defense Intelligence Agency operates a separate program for assessing SCI and SAP assets—critical and otherwise—but because its assessments are designed to focus on information security rather than mission assurance, they do not include certain key elements of those required for critical assets reported under DCIP. The Defense Intelligence Agency's guidelines for SCI and SAP assessments do not employ a mission-based analysis, nor do they require consideration of all potential hazards—whereas these two criteria are integral to the DCIP vulnerability assessments conducted on collateral-level assets. Should DCIP identify any of the critical SCI assets that are currently unidentified, the Defense Threat Reduction Agency would be able to assess those assets, as it has personnel who possess SCI clearances. However, Defense Threat Reduction Agency officials told us that because of the greater access restrictions placed on SAP data, they are unlikely to gain access to the highly sensitive, mission-related information needed to perform vulnerability assessments on SAP assets.

SCI and SAP Vulnerability Assessments Do Not Include Key Risk Management Elements

The significant differences in vulnerability assessments performed on SCI and SAP assets, as compared with those performed on collateral-level assets, impede DOD's ability to assure the availability of highly sensitive defense critical infrastructure. Table 2 compares DCIP assessment policies with those used for SCI and SAP assets.

Table 2: Comparison of DCIP, SCI, and SAP Vulnerability Assessment Policies

Attribute	DCIP Mission assurance assessments	SCI Information and physical security assessments	SAP Information and physical security assessments
Periodic assessment is required	✓	✓	✓
Assets are prioritized according to criticality	✓		
Assessment focuses on combatant command missions	✓		
Assessment addresses all hazards	✓		
Assessment has departmentwide visibility	✓		
Assessment includes plans for redundancy	✓		
Risk remediation actions must be reported	✓		

Source: GAO analysis of DOD data.

While DCIP risk management policies call for a mission-based, all-hazards approach for DOD’s critical assets, the *SCI Administrative Security Manual*¹⁶—DOD’s primary guide for protecting SCI and SAP data and material¹⁷—takes a contrasting approach that emphasizes the protection of information from unauthorized access. Specifically, the annual inspections of SCI and SAP facilities, conducted by program managers and the Defense Intelligence Agency, focus on information security rather than on mission assurance, and on human threats rather than on all potential hazards. These inspections are required to determine, for example, whether facilities regularly obtain threat assessments from a supporting law enforcement agency or counterintelligence office, but they are not required to verify the existence of threat assessments for natural disasters, accidents, public works or mechanical failure, or other diverse hazards. The manual also requires facilities to develop emergency action plans that outline policies, responsibilities, and procedures for protecting SCI and SAP material during emergencies. While these emergency action plans must consider a broad array of potential threats, they address only post-incident planning, and they do not discuss preventive measures, such as hardening facilities or enhancing redundancy. Unlike DCIP’s critical asset policy, moreover, SCI and SAP policy contains no requirement that asset owners or operators report to ASD(HD&ASA) or another body the actions they have taken, as a result of vulnerability assessments, to assure the availability of their assets. These fundamental differences prevent DOD from applying consistent and comprehensive risk management across all of its critical assets.

¹⁶ DOD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*, Defense Intelligence Agency (August 3, 1998) (For Official Use Only).

¹⁷ DOD officials responsible for SAP policy told us that SCI security standards, including the *SCI Administrative Security Manual*, are used to determine the baseline measures required to safeguard SAPs. The standards are then supplemented by measures described in the program security guides of each individual SAP.

DCIP Assessments Are Feasible for SCI, but Unlikely for SAP Assets

Performing an infrastructure vulnerability assessment requires an understanding of the asset's mission and operating characteristics, which in the case of SCI or SAP assets is available only to authorized individuals. The Defense Threat Reduction Agency has assessment staff who possess SCI clearances, which has enabled it to perform non-DCIP assessments of SCI assets in the past. Therefore, it could also assess vulnerabilities of SCI assets as part of DCIP, should any unidentified SCI assets be identified as critical under the program. Officials at the Defense Intelligence Agency told us that its SCI facility inspection teams currently do not coordinate with the Defense Threat Reduction Agency's DCIP assessment teams, but could feasibly do so.

Conversely, there have been no cases where Defense Threat Reduction Agency staff have been granted access to a SAP for the purpose of a vulnerability assessment, according to officials at the agency. Even if gaining access were possible, it might not be feasible. DOD officials responsible for SAP policy told us that the department operates more than 100 SAPs at any given time; vulnerability assessment staff would have to satisfy the individual access requirements of each SAP with critical infrastructure. Unless DOD develops a process for assessing SAP infrastructure that can satisfy DCIP standards and benchmarks while respecting the extraordinary sensitivity of SAP information, DOD will continue to lack sufficient information to make sound risk management decisions concerning critical SAP assets.

Conclusions

DOD has taken significant steps toward identifying, prioritizing, and assessing vulnerabilities of the DOD- and non-DOD-owned infrastructure it relies on to plan, mobilize, deploy, execute, and sustain U.S. military operations globally. Having a complete list of prioritized and assessed critical infrastructure will enable DOD to target limited resources to its most mission-critical assets at highest risk. However, DOD's current practice of limiting its data collection and analysis to collateral-level infrastructure has resulted in the exclusion of an undetermined number of critical SCI and SAP assets from the department's list of critical infrastructure. This exclusion creates risk management challenges, impeding DOD's ability to make informed decisions about potentially serious risks to core defense missions. Until DOD devises an integrated approach to identify, prioritize, and assess all of its critical infrastructure—collateral, SCI, and SAP assets—or develops parallel approaches that use mission-based, all-hazards criteria, DOD will lack the full awareness needed to assure mission success.

Recommendations for Executive Action

To ensure that DOD adequately identifies, prioritizes, and assesses critical SCI and SAP infrastructure, we recommend that the Secretary of Defense direct ASD(HD&ASA) to take the following two actions:

- Develop a process to identify, prioritize, and assess all critical SCI and SAP assets in a manner consistent with DCIP standards. As one option, ASD(HD&ASA) could partner with the Defense Intelligence Agency and the SAP Central Office to compile separate lists of, and to perform mission-based, all-hazards vulnerabilities assessments on, critical SCI and SAP assets.
- Amend the *DCIP Security Classification Guide* to explicitly address the treatment of SCI and SAP information on critical asset lists.

Agency Comments

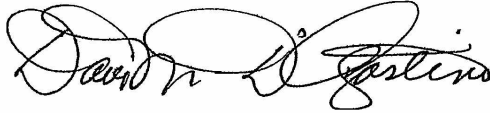
In written comments on a draft of this report, DOD concurred with one recommendation and partially concurred with the other. DOD's comments are reproduced in full in enclosure I. DOD also provided us with technical comments, which we incorporated where appropriate.

DOD partially concurred with our recommendation to develop a process to identify, prioritize, and assess all critical SCI and SAP assets in a manner consistent with DCIP standards. In its comments, ASD(HD&ASA) stated that it has begun working with its counterparts in the Defense Intelligence Agency and the SAP Central Office to formalize such a process. ASD(HD&ASA) also indicated that it plans to work with the Defense Threat Reduction Agency and the Defense Intelligence Agency on methodologies for assessing SCI assets. We believe that these two coordination efforts are necessary initial steps toward comprehensive risk management of DOD's highly sensitive critical infrastructure, and are consistent with the intent of our recommendation. Regardless of what approach it ultimately devises, as we recommended, DOD should ensure that it identifies and prioritizes all mission-critical SCI and SAP assets, and that it employs a mission-based, all-hazards analysis in assessing the assets' vulnerabilities.

DOD concurred with our recommendation to amend the *DCIP Security Classification Guide* to explicitly address the treatment of SCI and SAP information on critical asset lists. In collaboration with the Defense Intelligence Agency and the SAP Central Office, ASD(HD&ASA) will issue interim guidance on this subject, and subsequently incorporate that guidance into a new DOD manual to supersede the *Classification Guide*.

As agreed with your offices, we are sending copies of this report to the Chairmen and Ranking Members of the Senate and House Committees on Appropriations, Senate and House Committees on Armed Services, and other interested congressional parties. We also are sending copies of this report to the Secretary of Defense; the Secretary of Homeland Security; the Director, Office of Management and Budget; and the Chairman of the Joint Chiefs of Staff. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or by e-mail at dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in enclosure II.

A handwritten signature in black ink, appearing to read "Davi M. D'Agostino". The signature is fluid and cursive, with the first name "Davi" and last name "D'Agostino" clearly legible.

Davi M. D'Agostino
Director
Defense Capabilities and Management

Enclosures – 2

Comments from the Department of Defense



HOMELAND
DEFENSE

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

MAR 27 2008

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

This is the Department of Defense (DOD) response to the GAO draft report, GAO-08-373R, "DEFENSE CRITICAL INFRASTRUCTURE: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets," dated February 28, 2008 (GAO Code 351157). DOD concurs with comment on both recommendations in the report. Our response to your recommendations is attached.

Our point of contact for this action is Mr. Antwane Johnson, Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD (HD&ASA)), (703) 602-5730, Extension 143 or Antwane.Johnson@osd.mil.

Sincerely,

A handwritten signature in black ink that reads "P. McHale".

Paul McHale

Attachment:
As stated



**GAO DRAFT REPORT – DATED FEBRUARY 28, 2008
GAO CODE 351157/GAO-08-373R**

**“Defense Critical Infrastructure: DOD’s Risk Analysis of Its
Critical Infrastructure Omits Highly Sensitive Assets”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE RECOMMENDATIONS**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs (ASD(HD&ASA)) to develop a process to identify, prioritize, and assess all critical Sensitive Compartmented Information (SCI) and Special Access Program (SAP) assets in a manner consistent with the Defense Critical Infrastructure Program (DCIP) standards. As one option, ASD(HD&ASA) could partner with the Defense Intelligence Agency and the SAP Central Office to compile separate lists of, and to perform mission-based, all-hazards vulnerabilities assessments on, critical SCI and SAP assets.

DOD RESPONSE: Partially concur with comment. The DCIP Office is working with its counterparts in the Defense Intelligence Agency and the SAP Central Office to formalize a process that ensures that all critical Sensitive Compartmented Information (SCI) and Special Access Program (SAP) assets are identified, prioritized, and assessed by DOD as part of a comprehensive approach to risk management.

The Intelligence, Surveillance, and Reconnaissance (ISR) Sector, an oversight body reporting to the Director, Defense Intelligence Agency (DIA), has developed a list of SCI assets. The list of over 80 SCI assets was developed, coordinated, and approved by the membership of the ISR Sector Working Group, which includes the national agencies (National Security Agency (NSA), National Reconnaissance Office (NRO), and National Geospatial Intelligence Agency (NGA)), DIA, the Service intelligence activities, and Combatant Command J2 staffs. This aggregate list of prioritized SCI assets, classified at the TS/SCI level, is being managed by DIA.

As acknowledged by GAO, the Defense Threat Reduction Agency (DTRA) has an assessment staff who possess SCI clearances. DTRA has conducted Baseline Survivability Assessments (BSAs) and Full Spectrum Survivability Vulnerability Assessments (FSIVAs) at a variety of ISR Sector SCI assets including, among others, the national and defense intelligence agencies, the National Military Joint Intelligence Center (NMJIC), and several of the Command Headquarters, including their Intelligence Staff (J2). The DCIP Office will coordinate with DTRA and the ISR Sector regarding assessment methodologies.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs

(ASD(HD&ASA) to amend the *DCIP Security Classification Guide* to explicitly address the treatment of Sensitive Compartmented Information and Special Access Program information on critical asset lists.

DOD RESPONSE: Concur with comment. The DCIP Office, in collaboration with the DIA and the SAP Central Office will develop processes and procedures to explicitly address the treatment of Sensitive Compartmented Information and Special Access Program information on critical asset lists. OASD(HD&ASA) will issue interim guidance regarding the handling of SCI and SAP information on critical assets. This guidance will then be incorporated into a new DOD manual that will supersede the *DCIP Security Classification Guide*.

GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Acknowledgments

In addition to the contact named above, Mark A. Pross, Assistant Director; Jonathan K. Bateman; Katherine S. Lenane; Danielle S. Pakdaman; Terry L. Richardson; Marc J. Schwartz; and Cheryl A. Weissman made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.
