United States Government Accountability Office

GAO

Report to Congressional Requesters

August 2008

DEFENSE CRITICAL INFRASTRUCTURE

Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets

GAO-08-851

August 2008

DEFENSE CRITICAL INFRASTRUCTURE

Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-851, a report to congressional requesters

Why GAO Did This Study

The Department of Defense (DOD) established the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure, including surface, sea, and air transportation assets to carry out its missions. GAO was asked to evaluate (1) the extent to which the U.S. Transportation Command (TRANSCOM) has identified, prioritized, and assessed critical transportation assets; (2) the extent to which DOD installation personnel have taken actions to help assure the availability of critical transportation assets, both within and independent of DCIP; and (3) how DOD is funding critical transportation asset assurance. GAO examined a nonprojectable sample of 22 critical transportation assets, reviewed relevant DOD guidance and documents, and interviewed cognizant officials.

What GAO Recommends

GAO recommends TRANSCOM (1) implement established criteria to identify critical transportation assets, and develop a timeline for doing so, (2) discontinue its use of vulnerability assessments as its primary tool for identifying its critical assets, and (3) finalize an agreement with the Joint Staff to participate as transportation experts on Joint Staff DCIP vulnerability assessments, and that the military services develop and implement service-specific DCIP guidance. DOD partially concurred with the recommendations. GAO modified one recommendation on vulnerability assessments, in response to agency comments.

To view the full product, including the scope and methodology, click on GAO-08-851. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

What GAO Found

TRANSCOM has taken some actions to identify, prioritize, and assess its critical transportation assets but, according to officials from the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]), its methodology for doing so, until recently, has been inconsistent with the intent of DOD's various DCIP guidance and with the approach adopted by some of the other combatant commands and military services. TRANSCOM considers entire installations—military air bases, seaports, and commercial airports—as critical assets, rather than identifying assets with greater specificity, such as individual runways, navigation aids, and fuel storage facilities. This methodology diminishes the reliability of the critical transportation asset list, a condition that impedes DOD's ability to prioritize its critical assets departmentwide and effectively target spending on risk-reduction efforts. Further, TRANSCOM was using its vulnerability assessments to identify specific critical transportation assets on the installations. This practice conflicts with DOD's DCIP guidance not to use vulnerability assessments to identify critical assets. Though TRANSCOM officials stated that they now plan to discontinue this practice, they were unable to provide ASD(HD&ASA) or GAO with any documentation to confirm that this decision had occurred officially. Further, TRANSCOM's memorandum of understanding with the Joint Staff to participate as transportation subject matter experts on the Joint Staff's vulnerability assessments with a DCIP module is still in draft. In May 2008, TRANSCOM officials told GAO that they now plan to use the draft DCIP critical asset identification process to reevaluate its 300 identified critical transportation assets; however, a timeline to complete this has not yet been determined.

DOD installation personnel at the 22 sites GAO visited have taken actions to help assure the availability of critical transportation assets; however, these actions have routinely occurred independent of DCIP. Consequently, they do not consider the full spectrum of threats and hazards and they tend to focus on preventing mass personnel casualties instead of critical asset assurance. DCIP's impact at the installations where the assets are located was negligible because of the lack of service-specific guidance. This gap in guidance hinders installation personnel's ability to make informed risk management decisions based on asset criticality. Coordination efforts between installation personnel and non-DOD owners of critical transportation assets and supporting public works infrastructure were substantial, but have been focused on the protection of people and not on asset assurance.

DOD has allocated approximately $283 million for DCIP from fiscal years 2004 to 2008, including $8.6 million to TRANSCOM for its combatant command and defense sector responsibilities. Critical infrastructure assurance efforts also have been funded through other DOD complementary programs, such as the Antiterrorism Program, and through foreign government contributions. Although existing DCIP funding does not include funding for remediating asset vulnerabilities, remediation has been funded from these other sources.

Contents

Abbreviations

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
DCIP	Defense Critical Infrastructure Program
DOD	Department of Defense
OSD	Office of the Secretary of Defense
TRANSCOM	U.S. Transportation Command

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 15, 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 W. Todd Akin
House of Representatives

The Department of Defense (DOD) relies on a global network of critical surface, sea, and air transportation infrastructure—such as roads, railways, seaports, military air bases, and commercial airports—to carry out its missions. The incapacitation or destruction of one or more of the assets constituting this network of critical infrastructure could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. DOD's critical transportation infrastructure is owned by both DOD and non-DOD entities, including private companies, state and local governments, and foreign governments. Because of its importance to DOD operations, this critical infrastructure represents an attractive target to adversaries, and may also be vulnerable to a host of natural disasters and accidents. DOD has recognized and emphasized the importance of assuring the availability of mission-critical infrastructure in the most recent versions of the National Military Strategy[1] and the Quadrennial Defense Review.[2] Critical assets in the Transportation Defense Sector depend on public works infrastructure that provides the utilities needed for many transportation critical assets to remain

[1]Department of Defense, *The National Military Strategy of the United States of America: A Strategy for Today: A Vision for Tomorrow* (Washington, D.C.: 2004). The *National Military Strategy* is the Joint Chiefs of Staff's document on the strategic direction of the armed forces, which establishes three military objectives: (1) protect the United States against external attacks and aggression, (2) prevent conflict and surprise attack, and (3) prevail against adversaries.

[2]Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Feb. 6, 2006). The Quadrennial Defense Review is a comprehensive internal review of DOD's forces, resources, and programs.

operational.[3] To identify and help assure the availability of mission-critical infrastructure, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) was assigned responsibility for the risk-based Defense Critical Infrastructure Program (DCIP) in September 2003. ASD(HD&ASA) subsequently issued guidance in August 2005 articulating the roles and responsibilities for DOD organizations involved in the program.[4]

Under DCIP, DOD created 10 functionally based defense sectors and designated a Defense Infrastructure Sector Lead Agent (sector lead agent) for each sector.[5] The U.S. Transportation Command (TRANSCOM) is the sector lead agent for the Transportation Defense Sector. DOD Directive 3020.40 assigns the sector lead agent responsibility for, in collaboration with other DCIP stakeholders, identifying the interdependencies among infrastructure that crosses DOD sector boundaries, and for maintaining a characterization of sector support functions, systems, assets, and dependencies as they relate to identified operational capabilities and assets. Because TRANSCOM also is a combatant command, it is responsible for preventing and mitigating the loss of DOD-owned critical assets, within its assigned area of responsibility, and for coordinating with the military services and other sector lead agents in identifying and assessing critical assets. In addition to DCIP, DOD has established several other complementary programs, such as the Antiterrorism Program, that predate DCIP but contribute indirectly to the protection and assurance of critical assets.

You requested that we review a number of issues related to DOD's mission-critical infrastructure. To date, we have issued four reports in response to that request. Our first report examined the extent to which DOD has developed a comprehensive management plan for DCIP and the actions needed to identify, prioritize, and assess defense critical

[3]The purpose of public works infrastructure, according to the draft *DOD Critical Asset Identification Process* manual, is to provide and maintain utilities and real property and provide emergency services.

[4]DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)* (Washington, D.C.: Apr. 19, 2005).

[5]The 10 defense sectors are the Defense Industrial Base; Financial Services; Global Information Grid; Health Affairs; Intelligence, Surveillance, and Reconnaissance; Logistics; Personnel; Public Works; Space; and Transportation.

infrastructure.[6] The second report examined DOD's efforts to implement a risk management approach for defense industrial base critical assets.[7] The third report examined the extent to which DOD included highly sensitive assets in its critical infrastructure program.[8] Finally, the fourth report focused on threats and vulnerabilities affecting intelligence, surveillance, and reconnaissance operations at Creech Air Force Base, Nevada.[9] As agreed with your offices, we plan to issue two additional reports later this year. The first report evaluates DOD's efforts to assure the availability of critical infrastructure in the Space; Intelligence, Surveillance, and Reconnaissance; and Global Information Grid Defense Sectors.[10] The other report examines the extent to which DOD has trained key personnel and developed expertise to assist DOD organizations across five defense sectors in assuring the availability of critical infrastructure and has incorporated the assurance of critical infrastructure into exercises.

In 2007, we reported that DCIP implementation at the department, military service, and combatant command headquarters levels was relatively immature.[11] To understand what impact this was having on the availability of mission-essential transportation and supporting public works assets,[12] this report focuses on DOD and non-DOD (i.e., foreign) installations where the critical transportation assets are located. Specifically, we evaluated

[6]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).

[7]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).

[8]GAO, *Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets*, GAO-08-373R (Washington, D.C.: Apr. 2, 2008).

[9]GAO, *Defense Critical Infrastructure: Additional Air Force Actions Needed at Creech Air Force Base to Ensure Protection and Continuity of UAS Operations*, GAO-08-469RNI (Washington, D.C.: Apr. 23, 2008) (For Official Use Only).

[10]GAO, *Defense Critical Infrastructure: DOD's Evolving Assurance Program Has Made Progress but Leaves Critical Space, Intelligence, and Global Communications Assets at Risk*, GAO-08-828NI (For Official Use Only), forthcoming.

[11]GAO-07-461.

[12]While public works is one of the 10 defense sectors identified by ASD(HD&ASA) in DOD Directive 3020.40, assets in this defense sector did not rise to the same level of criticality as assets in other sectors. Because the Joint Staff list of Tier 1 critical assets does not include critical assets from the Public Works Defense Sector, for the purposes of this report, we are treating public works assets as supporting infrastructure.

Critical asset tiers

- **Tier 1**—An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DOD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level.
- **Tier 2**—An asset the loss, incapacitation, or disruption of which could result in mission (or function) degradation at the DOD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level.
- **Tier 3**—An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure below the military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level.

(1) the extent to which TRANSCOM has identified, prioritized, and assessed its critical transportation assets; (2) the extent to which DOD installation personnel have taken actions to help assure the availability of critical transportation assets, both within and independent of DCIP; and (3) how DOD is funding critical transportation asset assurance.

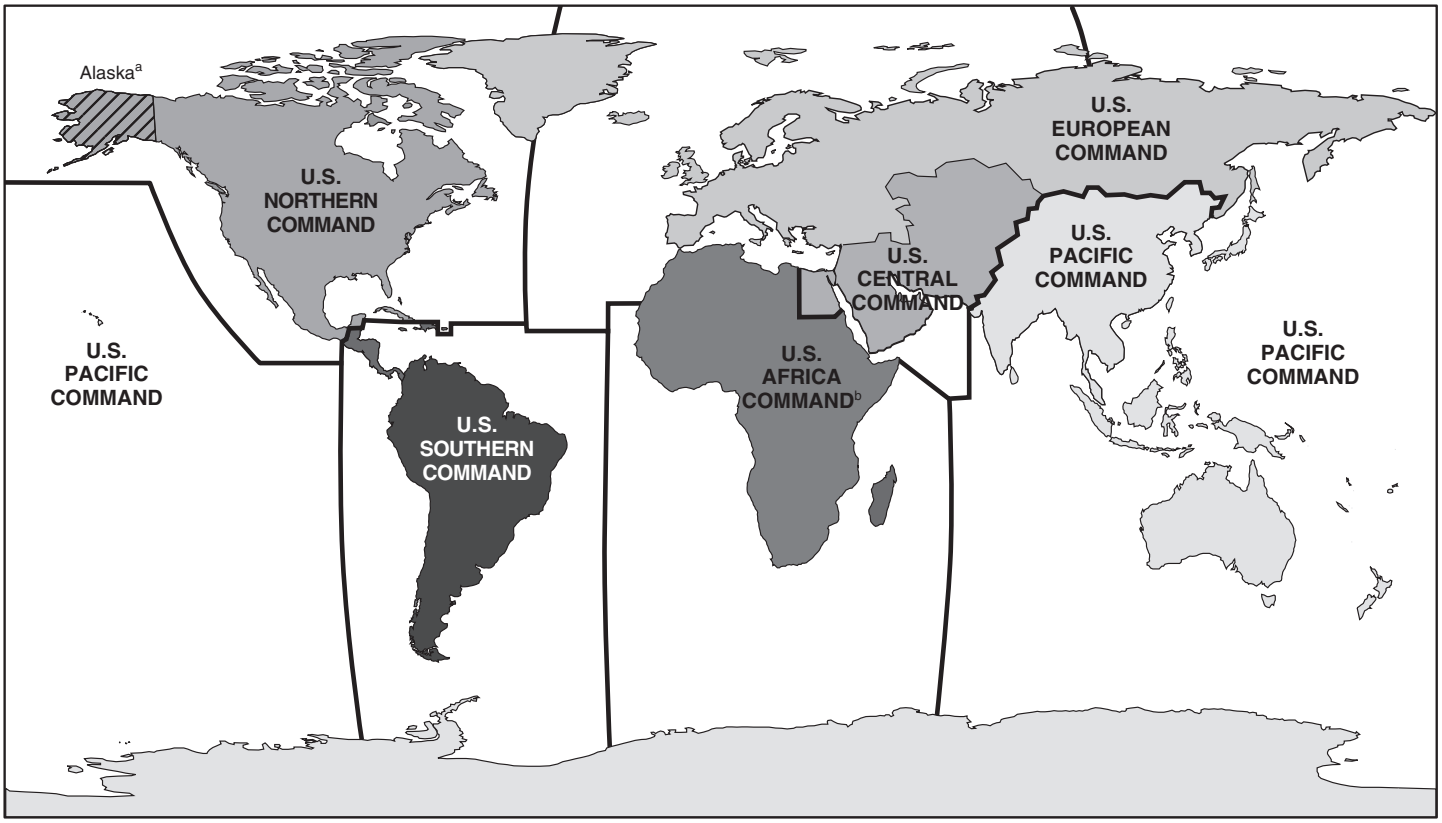
We drew a nonprobability sample[13] of critical transportation assets in the United States and abroad, using draft critical asset lists developed by the Joint Staff, each of the four military services, and TRANSCOM. We selected assets based on (1) overlap among the various critical asset lists; (2) geographic dispersion among geographic combatant commands' areas of responsibility; (3) representation from each military service; and (4) representation in the three asset categories—air bases, seaports, and commercial airports—TRANSCOM identified in the continental United States, and in the European, Middle Eastern, and Pacific regions. Through this methodology, we selected 22 assets for review, including two of the four Tier 1 critical transportation assets.[14] Tier 1 assets represent those assets that are most critical for carrying out combatant command missions.

Figure 1 shows the areas of responsibility for each geographic combatant command.

[13]Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studied have no chance or an unknown chance of being selected as part of the sample.

[14]At the time of our sample selection, only four transportation assets had been identified as Tier 1 critical assets; however, TRANSCOM subsequently identified four more, raising the total to eight Tier 1 critical transportation assets. Of these eight assets, two were included in our sample.

Figure 1: Geographic Combatant Commands' Areas of Responsibility



Source: GAO presentation of DOD data.

[a]The state of Alaska is assigned to the U.S. Northern Command's area of responsibility. Forces based in Alaska, however, may be assigned to multiple commands.

[b]The U.S. Africa Command was officially established in October 2007 with a goal to reach full operational capability as a geographic combatant command by September 30, 2008, assuming responsibility for U.S. military activities in Africa.

Further, we assessed relevant planning documents, including continuity of operations and emergency management plans for assets we selected for review and for the associated public works assets that support them. We reviewed Transportation Infrastructure Vulnerability Assessments that focus on critical infrastructure, when available, for those DOD and foreign installations we visited. Also, we analyzed relevant Office of the Secretary of Defense (OSD), military service, and combatant command guidance and funding data. Within DOD, we interviewed officials from OSD, the Joint Staff, defense agencies, the military services, combatant commands, subcomponent commands, sector lead agents, and installation-level organizations in the United States and abroad. In addition, we interviewed

officials at the Department of Homeland Security, at three U.S. embassies and three commercial airports; host nation officials; and officials in both the private sector and academia. (Throughout this unclassified report, we do not identify specific assets, their locations or installations, or combatant command or others' missions that the assets support because that information is classified.) We conducted this performance audit from May 2007 through July 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. To assess the reliability of data, we interviewed appropriate officials and reviewed relevant documentation. We found the data provided by DOD to be sufficiently reliable for representing the nature and extent of the DCIP funding. A more thorough description of our scope and methodology is provided in appendix I.

Results in Brief

Although TRANSCOM has taken some actions to identify, prioritize, and assess its critical transportation assets, its methodology for doing so, until recently, has been, according to ASD(HD&ASA) officials, inconsistent with the intent of DCIP guidance and with the approach adopted by some of the other combatant commands and military services. TRANSCOM has identified entire installations—military air bases, seaports, and commercial airports—as critical assets, rather than identifying critical assets with greater specificity, such as individual runways, navigation aids, and fuel storage facilities. TRANSCOM officials identified entire installations based on their interpretation of the definition of an asset as outlined in DOD Directive 3020.40 and because these types of installations constitute the worldwide Defense Transportation System necessary to carry out TRANSCOM's missions. This methodology of identifying critical assets diminishes the reliability of the critical transportation asset list, a condition that impedes DOD's ability to prioritize its critical assets and effectively target spending for risk reduction efforts. TRANSCOM was using its Transportation Infrastructure Vulnerability Assessments to identify specific critical transportation assets on the installations, a practice that conflicts with DOD's DCIP guidance not to use vulnerability assessments for this purpose. Though TRANSCOM officials stated that they now plan to discontinue this practice, they were unable to provide ASD(HD&ASA) or us with any documentation to confirm that this decision had occurred officially. Further, TRANSCOM's memorandum of understanding with the Joint Staff to participate as transportation subject

matter experts on the Joint Staff's vulnerability assessments with a DCIP module is still in draft. In May 2008, TRANSCOM officials told us that they now plan to use the draft DCIP critical asset identification process to reevaluate its critical transportation assets. TRANSCOM officials believe that this will result in a "significant reduction" in the number of assets it identifies as critical; however, TRANSCOM has not yet set a timeline to begin and complete this reevaluation.

DOD installation personnel have taken actions to help assure the availability of critical transportation assets. However, because the vast majority of these actions have occurred outside of DCIP, their actions do not consider the full spectrum of threats and hazards, and tend to focus on preventing mass personnel casualties instead of assuring asset availability. Although DOD established DCIP to help assure the availability of critical infrastructure—including transportation assets—departmentwide, DCIP's impact at the 22 installations we visited where the assets were located was negligible. For 18 of the 22 critical transportation assets we examined, we found that (1) installation personnel were often unaware of the criticality of their assets for TRANSCOM's missions and (2) coordination efforts between installation personnel and DOD and non-DOD owners of critical transportation assets and their supporting public works infrastructure were substantial, but again tended to focus on the protection of people and not on ensuring the availability of critical assets. DCIP guidance instructs the military departments to allocate resources for an organizational program supporting DCIP, including the implementation of risk management decisions. Further, it requires combatant commands to coordinate with other combatant commands, the military services, and sector lead agents in identifying and assessing critical assets and associated infrastructure interdependencies and to act to prevent or mitigate loss or degradation of critical assets. However, at 20 of the 22 installations we visited, critical assets were not incorporated into installations' emergency management, continuity of operations, or risk management plans. Further, installation personnel attributed their unfamiliarity with DCIP to the military services not yet having issued DCIP implementing guidance as well as the frequent rotations of installation commanders. As a result, this gap hindered installation personnel's ability to make informed risk management decisions, such as remediation priorities, because installation personnel at the sites we visited were not aware of what assets were more critical than others.

DOD has allocated approximately $283 million in budgeted and supplemental appropriations for critical asset assurance through DCIP from fiscal years 2004 to 2008, including about $8.6 million to TRANSCOM. DCIP guidance requires combatant commands and sector lead agents to provide adequate resources to implement their DCIP responsibilities. To this end, TRANSCOM has allocated approximately $5.7 million for its combatant command DCIP responsibilities and $2.9 million for its Transportation Defense Sector DCIP responsibilities during this 5-year period to identify and assess its critical assets. Additionally, asset owners have funded critical asset initiatives through other DOD programs, such as the Antiterrorism Program, as well as benefited from funding from foreign government payments in countries where DOD has identified critical transportation assets. Although existing DCIP funding does not include funding for remediation of critical asset vulnerabilities, some remediation has occurred through these other complementary programs.

We are recommending that TRANSCOM fully implement the criteria, methodology, and process in the draft *DOD Critical Asset Identification Process* manual to reevaluate and update the identification of all critical transportation assets, and develop a timeline for doing so; discontinue the use of Transportation Infrastructure Vulnerability Assessments as its primary tool for identifying its critical assets; and finalize the memorandum of understanding with the Joint Staff to enable TRANSCOM transportation subject matter experts to participate in the DCIP module of a Joint Staff vulnerability assessment. Also, we are recommending that the military departments develop and implement service-specific guidance based on published DOD DCIP guidance.

GAO provided a draft of this report to DOD in July 2008 with three draft recommendations for its review and comment. In written comments on a draft of this report, DOD partially concurred with our recommendations. Based on DOD's agency comments, we modified one recommendation (making it two recommendations rather than one) to reflect the distinction between the separate issues of finalizing the memorandum of understanding with the Joint Staff and discontinuing the use of Transportation Infrastructure Vulnerability Assessments as the primary tool to identify critical assets. Also, TRANSCOM and U.S. Central Command provided us with technical comments, which we incorporated in the report as appropriate. DOD's response is reprinted in appendix II.

Background

Homeland Security Presidential Directive 7,[15] issued in December 2003, designates the Secretary of Homeland Security as the principal federal official responsible for leading, integrating, and coordinating the overall national effort to protect the nation's critical infrastructure and key resources. *Homeland Security Presidential Directive 7* also requires all federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources from terrorist attacks. ASD(HD&ASA), within the Office of the Under Secretary of Defense for Policy, serves as the principal civilian advisor and the Chairman of the Joint Chiefs of Staff serves as the principal military advisor to the Secretary of Defense on critical infrastructure protection.

The Transportation Defense Sector is made up of a worldwide network of DOD and non-DOD surface, sea, and air assets that the U.S. military relies on to move personnel and equipment. Currently, the Transportation Defense Sector consists of 300 critical air bases, seaports, and commercial airports worldwide and owned by DOD, other U.S. governmental organizations, private companies, and foreign governments. According to TRANSCOM officials, the Transportation Defense Sector is highly resilient because of significant redundancy among the various modes of transportation, particularly as it relates to surface transportation. For example, the size and capabilities of the U.S. rail and highway networks afford ability to reroute shipments via alternate roads and rail lines in the event of disruptions, a key reason why surface transportation assets were not identified as critical.

In addition to DCIP, DOD has established other complementary programs that help assure critical assets, including the Antiterrorism Program[16] and the Defense Continuity Program.[17] The Antiterrorism Program is intended to establish protection standards for DOD assets against terrorist attacks. The Defense Continuity Program is intended to ensure that DOD mission-essential functions continue under all circumstances, such as a man-made or natural disaster. DCIP supports a risk-management process that seeks to ensure defense critical infrastructure availability. The risk-management process is comprised of a risk assessment component that identifies

[15]*Homeland Security Presidential Directive 7* (Washington, D.C.: Dec. 17, 2003).

[16]DOD Directive 2000.12, *DOD Antiterrorism (AT) Program* (Washington, D.C.: Dec. 13, 2007).

[17]DOD Directive 3020.26, *Defense Continuity Program (DCP)* (Washington, D.C.: Jan. 1, 2007).

critical assets and infrastructure interdependencies that support DOD missions. Applicable follow-on threat and vulnerability assessments are then conducted on those assets to complete the risk assessment. The risk response component ensures that limited resources are optimally allocated towards those assets deemed most important to overall mission success for DOD, and for which it has been determined that the identified level of risk is unacceptable.

Several DOD organizations have key roles in helping assure the availability of DOD's transportation critical assets. The military services, defense agencies, and the combatant commands are responsible, in coordination with the sector lead agents, for identifying and assessing critical assets. The military departments, in their role as executive agent for the combatant commands, provide funding and resources for combatant command critical infrastructure programs. DOD Directive 3020.40 also states that sector lead agents are responsible for collaborating with other defense sector lead agents and DOD DCIP stakeholders to identify cross-sector interdependencies.

TRANSCOM Efforts to Identify, Prioritize, and Assess Critical Transportation Assets Have Been Inconsistent with Guidance

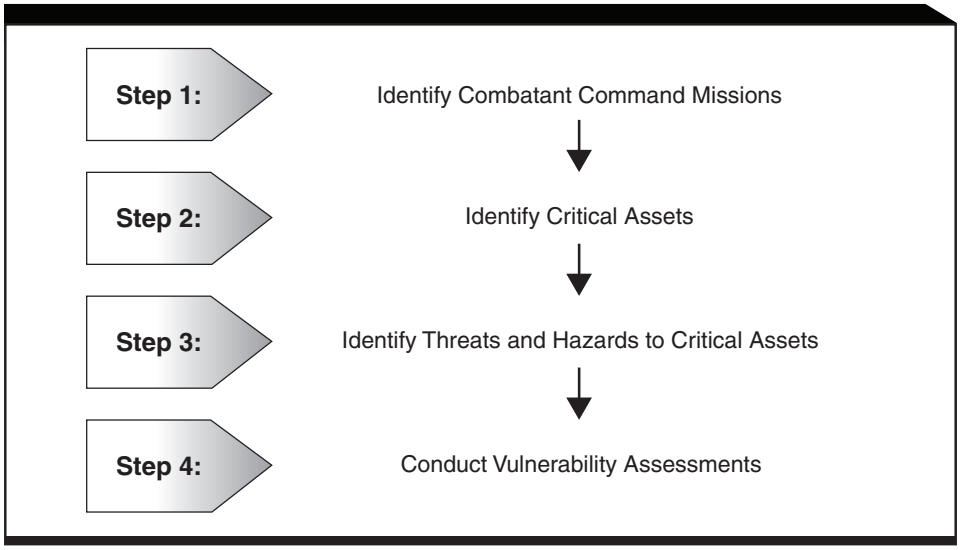
According to ASD(HD&ASA) officials, TRANSCOM's methodology for identifying, prioritizing, and assessing its critical transportation assets is inconsistent with the intent of DOD's DCIP guidance and with the approach adopted by some of the other combatant commands and military services. TRANSCOM officials stated in May 2008 that they now plan to leverage the draft *DOD Critical Asset Identification Process* manual to reevaluate its currently identified critical transportation assets; however, a timeline to complete this reevaluation has not yet been established. Further, until recently, TRANSCOM relied on its vulnerability assessments to identify critical transportation assets, an action that also conflicted with established DOD guidance and practice. While TRANSCOM officials stated that they will discontinue the use of vulnerability assessment for identification purposes, they were unable to provide any documentation to ASD(HD&ASA) or us to confirm this decision officially. Moreover, its memorandum of understanding with the Joint Staff to participate as transportation subject matter experts on Joint Staff DCIP vulnerability assessments is still in draft.

TRANSCOM's Asset Identification Efforts Are Inconsistent with Intent of DCIP Guidance and Practice

At the time of our review, TRANSCOM had identified 300 Tier 1 and Tier 2 critical transportation assets linked to its global mobility mission. TRANSCOM officials told us that they identified larger systems of assets—categorized as air bases, seaports, and commercial airports—based on their interpretation of the definition of an asset as outlined in DOD Directive 3020.40.[18] TRANSCOM officials explained that these types of installations are part of its worldwide Defense Transportation System that is necessary to carry out TRANSCOM's missions. This broad list of assets has been submitted to the Joint Staff for inclusion in DOD's overall draft critical asset list. Because of TRANSCOM's interpretation of the guidance, its critical asset list lacks the specificity of the critical asset lists prepared by some of the other combatant commands and military services. Moreover, according to ASD(HD&ASA) officials, TRANSCOM's decision to identify entire installations was inconsistent with the intent of DCIP guidance. While TRANSCOM is not the only combatant command or military service to identify an entire installation as critical, it is the only organization that has done so for its entire list. DOD guidance requires combatant commands to first identify their missions, the critical assets that support those missions, and the threats and hazards to those critical assets, and then assess the vulnerability of the critical assets to the threats and hazards identified (see fig. 2).

[18]DOD Directive 3020.40 defines an asset as a distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public, or private sector organizations.

Figure 2: DOD Guidance for Risk Management[19]



Source: GAO analysis of DOD data.

TRANSCOM skips steps two and three listed in figure 2 and instead has been using Transportation Infrastructure Vulnerability Assessments to identify specific critical assets. According to TRANSCOM officials, the identification of threats and hazards to critical assets (step 3) is incorporated in the conduct of vulnerability assessments (step 4), since Transportation Infrastructure Vulnerability Assessments specifically address vulnerability to all threats and hazards.

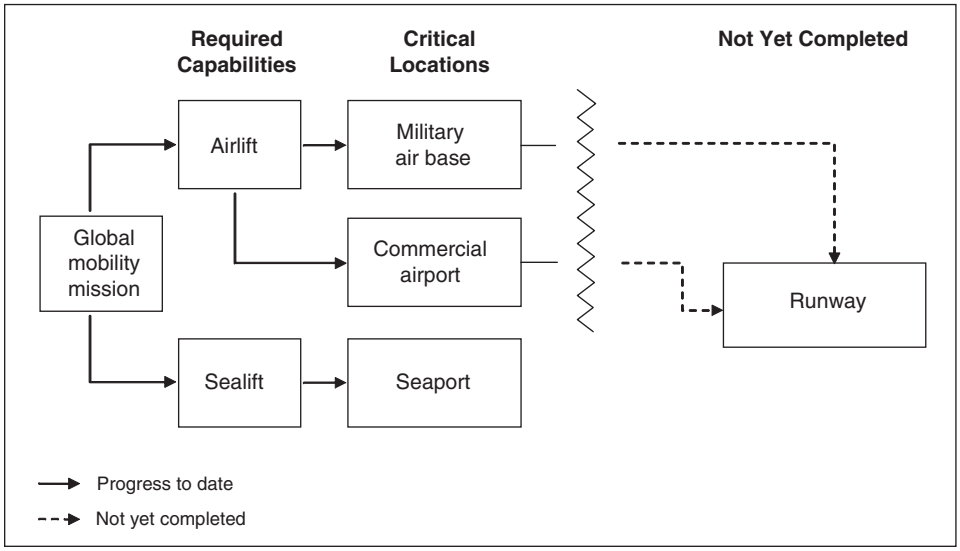
ASD(HD&ASA) officials stated that when they began developing an overall DOD critical asset list, they told the combatant commands and military services that stopping the identification process for critical assets at the installation level is insufficient for the purposes of DCIP. As a result of continued submission of entire installations as critical assets, ASD(HD&ASA) published in March 2008 the *Strategy for Defense Critical Infrastructure*[20] to reiterate the need for greater specificity in critical asset identification. Further, ASD(HD&ASA) is developing the *DOD Critical*

[19]DOD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, (Washington, D.C.: Apr. 21, 2008).

[20]DOD, ASD(HD&ASA), *Strategy for Defense Critical Infrastructure* (Washington, D.C.: Mar. 2008).

Asset Identification Process manual, which is still in draft, but also notes that stopping the asset identification process at the system level (e.g., an air base, seaport, or commercial airport) does not meet the needs of DCIP, and that rarely is an entire system essential to mission success. For example, it is insufficient to identify an air base as a critical asset; rather, more specific assets, such as a runway, should be identified as appropriate. Figure 3 illustrates the DCIP critical asset identification process and where TRANSCOM's previous efforts have stopped.

Figure 3: TRANSCOM's Efforts Prior to Implementing DCIP's Asset Identification Process



Source: GAO analysis of DOD data.

TRANSCOM officials stated that because the *DOD Critical Asset Identification Process* manual was still in draft, they had initially chosen not to implement its contents until its formal publication. According to TRANSCOM officials, beginning in May 2008, TRANSCOM began the process to develop coordination methods to facilitate the use of the criteria in the draft *DOD Critical Asset Identification Process* manual for the identification and validation of assets prior to submitting them to the Joint Staff. TRANSCOM has recognized that this process will require time to complete a meaningful critical transportation asset list; however, a timeline to complete this process has not yet been established.

Complicating the process of identifying and prioritizing critical assets has been TRANSCOM's use of Transportation Infrastructure Vulnerability

Assessments. Though contrary to DCIP guidance,[21] TRANSCOM has been using its vulnerability assessments to identify specific critical assets rather than using the process outlined in DCIP guidance to identify specific critical assets. As a result, TRANSCOM officials could not tell us what specific transportation assets at a given site were critical, stating that in the absence of a Transportation Infrastructure Vulnerability Assessment it could be, though not necessarily, assumed that what was identified as critical at one location might be critical at another. For example, if a Transportation Infrastructure Vulnerability Assessment identified specific critical assets (such as a runway, navigation aids, or a fuel depot) at an air base as critical, it could be reasonably assumed that the same assets would probably be critical at other air bases. However, while TRANSCOM officials have stated that they will discontinue the use of vulnerability assessment for identification purposes, they were unable to provide any documentation to ASD(HD&ASA) or us to confirm this decision officially. Additionally, TRANSCOM's memorandum of understanding with the Joint Staff to serve as transportation subject matter experts for the enhanced DCIP module to the Joint Staff's Integrated Vulnerability Assessment when transportation assets are assessed remains in draft.

At the behest of ASD(HD&ASA) in 2006, the Joint Staff began the process of creating a list of Tier 1 critical assets based on assets nominated and submitted by DOD organizations, including the combatant commands and the military services using DCIP-approved criteria. The Joint Staff's list has gone through several iterations and a subset of Tier 1 critical assets, known as Defense Critical Assets, will be selected by ASD(HD&ASA).[22] These Defense Critical Assets are of such extraordinary importance to DOD operations in peace, crisis, and war that their incapacitation or destruction would have a very serious, debilitating effect on the ability of DOD to fulfill its missions. TRANSCOM has not yet established a timeline to reevaluate critical transportation assets using the approved DCIP methodology. Until this reevaluation is completed, ASD(HD&ASA)'s ability to formulate a comprehensive Defense Critical Asset list that includes transportation assets and effectively targets spending for risk reduction efforts will be impeded.

[21]DOD Instruction 3020.45.

[22]According to DOD Instruction 3020.45, ASD(HD&ASA) is responsible for issuing a list of Defense Critical Assets based on nominations from the Chairman of the Joint Chiefs of Staff.

Figure 4 illustrates the types of specific critical transportation assets that TRANSCOM could identify below the installation (air base, seaport, and commercial airport) level.

Figure 4: Representative Types of Critical Transportation Assets

Cargo handling equipment at a U.S. air base.

Fuel transfer pipeline.

A refueling pier critical to sealift port operations.

Mobile control tower; a backup capability for continuity of air operations.

Source: DOD.

TRANSCOM plans to reevaluate its critical asset list using the DCIP-approved criteria, which is expected to result in a "significant reduction" of critical transportation assets.

Most Installations Took Some Steps to Assure the Availability of Critical Transportation and Public Works Assets but Were Unaware of Asset Criticality and Lacked a DCIP Focus

Although DOD established DCIP to help assure the availability of mission-critical infrastructure—including transportation assets—installation personnel were often unfamiliar with DCIP and unaware of the critical role specific transportation assets play in TRANSCOM's missions. This lack of awareness contributed to a singular focus on protecting personnel and did not consider mission-critical assets.

Installation Officials Often Are Unaware of Asset Criticality

Installation officials responsible for critical transportation assets at the 22 sites we visited were often unaware of asset criticality because they were unfamiliar with DCIP and thus DCIP's impact at these installations was negligible. While some efforts have been made to coordinate with both DOD and non-DOD entities, including the private sector, state and local governments, and foreign governments to assure the availability of critical transportation assets at home and abroad, these coordination efforts have been conducted despite a lack of service-specific DCIP implementation guidance. According to officials at 17 of the 22 installations we visited, efforts at installations have mostly focused on protecting people through such actions as antiterrorism protection rather than focusing on specific mission-critical transportation assets.

At 18 of the 22 installations we visited, we found numerous complementary programs, such as the Antiterrorism and Chemical, Biological, Radiological, Nuclear, and high-yield Explosive Programs; and continuity of operations and emergency management planning. Officials responsible for assuring the availability of critical transportation assets at 20 of the 22 installations we visited, told us that they had not heard of DCIP prior to our visit because (1) there is an absence of service-specific guidance that explains how to implement DCIP and (2) the frequent rotation of installation commanders (typically every 2 years), which can limit leadership continuity over DCIP at the installation level. Officials at 16 of the 22 installations we visited told us that they would have more vigorously advocated for resources to fund protection of critical assets had they been aware of an asset's criticality to TRANSCOM's mission.

Without service-specific guidance to ensure that mission-critical assets are being protected, installations rely on other complementary programs in lieu of the all-hazards approach[23] that DCIP requires.

Installation Coordination Efforts Have Been Extensive, but Often Do Not Focus on the Assurance of Mission-Critical Assets

Nearly all of the installations (18 of 22) we visited had coordinated with both DOD and non-DOD entities, including the private sector, state and local governments, and foreign governments to help assure the availability of critical transportation assets at home and abroad. However, these coordination efforts have been performed independent of DCIP and, therefore, focus on protecting people and not on assuring the availability of mission-critical transportation assets. DOD DCIP guidance requires the combatant commands to coordinate with one another and with the military services and sector lead agents to identify and assess critical assets. At 21 of the 22 sites we visited, installation officials had taken steps to coordinate such efforts with DOD organizations on the installation and/or with the private sector, state and local communities, or with host nation officials. For example, at one air base we visited in Europe, installation officials conducted joint security patrols with host nation military officials and trained jointly with military and civilian firefighting personnel. Further, at 10 DOD installations we visited in the Pacific region, installation officials routinely coordinated with state, local, and foreign governments on emergency management planning or scenarios, such as typhoons and earthquakes. Such coordination efforts, however, do not directly assure the availability of specific critical assets in the wake of a natural or man-made disaster.

Installations Have Taken Steps to Mitigate the Potential Disruption of Public Works

To mitigate public works disruptions, personnel at 18 of the 22 installations we visited were coordinating with DOD organizations on the installation, as well as local, state, or host nation officials. Specifically, these installations had developed resiliency in supporting public works infrastructure, such as fuel and electric power sources, so that critical transportation assets remained operational in the event of an installation-wide disruption. For example, 18 of these installations have developed backup or alternative capabilities to mitigate the loss of electricity and fuel. For 17 of the 22 critical transportation assets we visited, installation

[23] An all-hazards approach looks not only at intentional threats, such as hostile or terrorist attack, but also non-intentional hazards, such as accidents, weather events, and natural disasters.

personnel were coordinating with DOD tenant organizations on the installation and with host governments to maintain and sustain public works support for its assets located on the facility. Most of the installations we visited (17 of 22) had emergency management plans and continuity of operations plans that accounted for the loss or degradation of supporting public works infrastructure located on or within the installation, although none of the plans specifically identified the critical transportation assets as high-priority assets vis-à-vis the installation's other assets. We also found that installation personnel at 18 of the 22 locations we visited frequently tested and maintained backup fuel and electric power sources and often included them in their emergency management planning exercises. Seventeen of these installations had developed prioritized facilities lists to determine which facilities or assets would receive priority for power restoration when power to the installation was interrupted.

Critical Transportation Asset Assurance Has Received Some Funding through DCIP and Has Benefited from Other Sources of Funding

DOD has allocated approximately $283.3 million for critical asset assurance through DCIP from fiscal years 2004 to 2008. DCIP guidance requires combatant commands and sector lead agents to provide adequate resources to implement their DCIP responsibilities. TRANSCOM has received approximately $8.6 million over this period to carry out its DCIP responsibilities, both as a combatant command and as a sector lead agent for the Transportation Defense Sector. In addition to these funds, critical transportation assets also have benefited indirectly from other DOD programs, such as the Antiterrorism Program, and from funding from foreign governments in countries where the United States maintains a military presence.

Of the $8.6 million TRANSCOM has received in total DCIP funding from fiscal years 2004 to 2008, approximately $5.7 million has been used for carrying out its combatant command responsibilities and approximately $2.9 million has been used for implementing its transportation defense sector responsibilities.

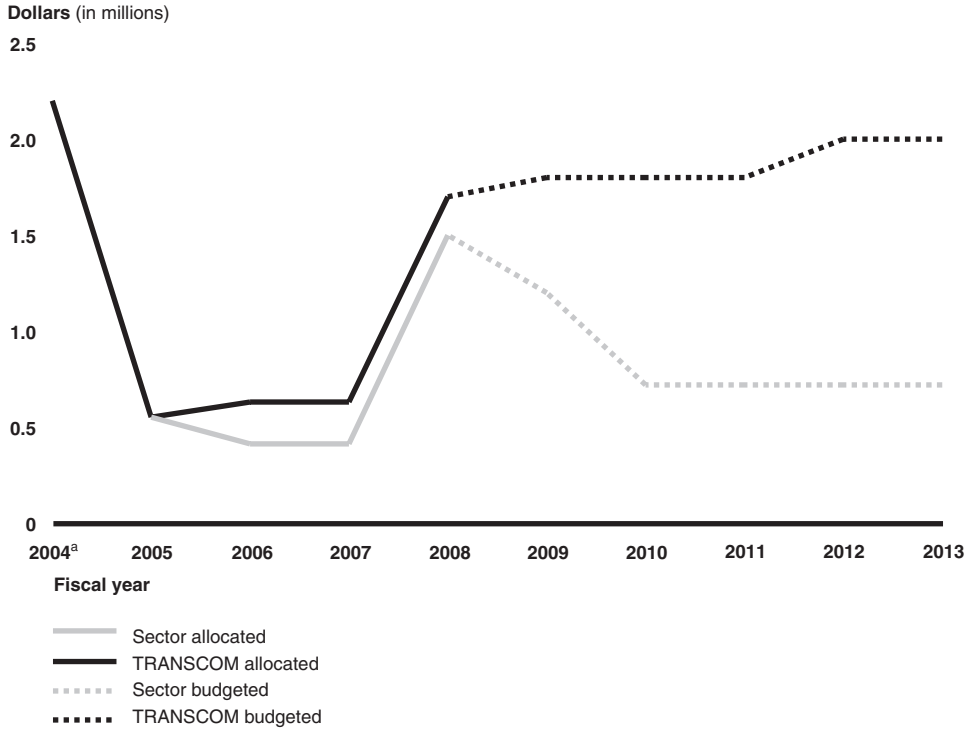
TRANSCOM, which is funded by the Air Force, as TRANSCOM's executive agent, has requested DCIP funding for fiscal years 2009 to 2013 totaling

$9.4 million for its combatant command responsibilities and $4.1 million[24] for its defense sector responsibilities. Although the Air Force has not established a dedicated funding account for DCIP for itself,[25] according to TRANSCOM officials, the Air Force has budgeted DCIP funding for TRANSCOM to perform its combatant command and defense sector responsibilities. Figure 5 depicts TRANSCOM's DCIP allocated and planned funding for its combatant command and defense sector responsibilities from fiscal years 2004 to 2013.

[24]According to TRANSCOM officials, ASD(HD&ASA) will continue to fund the Transportation Defense Sector at an average of $720,000 per year until fiscal year 2013 at which time TRANSCOM will be required to seek funding for its defense sector responsibilities from the Air Force, TRANSCOM's executive agent.

[25]A February 2006 memorandum from the Principal Deputy for ASD(HD&ASA) stated that beginning in fiscal year 2008, each service should allocate $2.4 million per year and each combatant command, through its executive agent, should allocate $1.8 million per year to carry out their assigned DCIP responsibilities.

Figure 5: TRANSCOM's DCIP Funding Trend, Fiscal Years 2004 to 2013



Source: GAO analysis of DOD data.

[a]Sector-specific funding data are unavailable for fiscal year 2004.

The assurance of critical transportation assets also benefits, indirectly, from other DOD sources, such as the Antiterrorism Program and the Combating Terrorism Readiness Initiative Fund. Among other things, the Antiterrorism Program provides a source of funding for installations to remediate vulnerabilities to transportation assets. Typically, remediation actions, such as improved security at entry control points or the hardening of a building to withstand an explosive blast, are done to counter a perceived terrorist threat—and do not explicitly consider other threats and hazards. Nonetheless, critical assets located within the installation or within a hardened building will benefit as a result of these other efforts. Further, the Combating Terrorism Readiness Initiative Fund provides another mechanism to fund antiterrorism measures, which tangentially affects the assurance of critical transportation assets.

In addition to other DOD programs, foreign countries that host the U.S. military fund initiatives that indirectly help assure critical transportation

assets. For example, U.S. embassy officials estimate that one country we visited in U.S. Central Command's area of responsibility provides over $1 billion annually and one country we visited in U.S. Pacific Command's area of responsibility contributes about $4.1 billion annually in support of the U.S. military presence in its country. In both instances, a portion of the funding contributed by these countries is used to safeguard installations containing critical transportation assets.

Conclusions

Until now, TRANSCOM's practice of designating entire air bases, seaports, and commercial airports as critical transportation assets has been inconsistent with DCIP guidance and the approach adopted by some of the other combatant commands and military services to identify specific mission-critical assets. Recently, however, TRANSCOM decided to discontinue its current critical asset identification process in favor of the draft critical asset identification methodology. TRANSCOM's decision will necessitate reevaluating the approximately 300 installations on its existing critical asset list—an undertaking that could potentially delay ASD(HD&ASA)'s issuance of the department's approved Defense Critical Asset List. Consequently, it is important for TRANSCOM to establish a timeline and key dates associated with the reevaluation process so that ASD(HD&ASA) can account for transportation assets in future iterations of the Defense Critical Asset List. Once this process is completed, ASD(HD&ASA) should have greater visibility over the full complement of mission-critical infrastructure and be better positioned to effectively remediate vulnerabilities to its most critical assets. While TRANSCOM officials have stated that they will discontinue the practice of using Transportation Infrastructure Vulnerability Assessments to identify specific critical transportation assets on the installations, they were not able to provide ASD(HD&ASA) or us with any documentation to confirm this decision officially. Lastly, until TRANSCOM finalizes its memorandum of understanding with the Joint Staff, it will not be able to define the roles and responsibilities of transportation subject matter experts to participate in the Joint Staff vulnerability assessments with a DCIP module.

Although OSD issued department-wide guidance on critical infrastructure in 2005, knowledge of the program at the installation level—where critical transportation assets are located—is minimal because the military services have not yet developed their own implementation guidance. This lack of awareness has led installation officials to rely on other, more established programs to protect critical assets. While programs, such as DCIP and the Antiterrorism Program, do share some precepts, there are significant differences in the types of threats and hazards each program focuses on

and in their emphasis on protection, resilience, and restoration of operations and assets. Until the military services issue guidance that installation personnel can use to implement local critical infrastructure programs, mission-critical assets may incur unintended risk.

Recommendations for Executive Action

We are making the following four recommendations to help assure the availability of critical assets in the Transportation Defense Sector.

To enable decision makers within DOD to more effectively prioritize and target limited resources to reduce critical asset vulnerabilities and allow ASD(HD&ASA) to formulate a complete and accurate list of Defense Critical Assets, we recommend that the Secretary of Defense, through ASD(HD&ASA) and the Chairman of the Joint Chiefs of Staff, direct the Commander of TRANSCOM to take the following three actions:

- Fully implement the criteria, methodology, and process in the draft *DOD Critical Asset Identification Process* manual to reevaluate and update the identification of all critical transportation assets, and develop a timeline for doing so.
- Discontinue the use of Transportation Infrastructure Vulnerability Assessments as its primary tool for identifying its critical assets.
- Finalize its memorandum of understanding with the Joint Staff to enable TRANSCOM transportation subject matter experts to participate in the DCIP module of a Joint Staff vulnerability assessment.

To facilitate DCIP implementation at the installation level, we recommend that the Secretary of Defense direct the secretaries of the military departments to develop and implement service-specific guidance based on published DOD DCIP guidance.

Agency Comments and Our Evaluation

In written comments on a draft of this report, which included three draft recommendations, DOD partially concurred with our recommendations. Also, TRANSCOM and U.S. Central Command provided us with technical comments, which we incorporated in the report where appropriate. DOD's comments are reprinted in appendix II.

In its written comments, DOD stated that it partially concurred with our recommendation that TRANSCOM fully implement the criteria, methodology, and processes outlined in the draft *DOD Critical Asset Identification Process* manual to reevaluate and update the identification

of all critical transportation assets, and develop a timeline for doing so. DOD agreed with the recommendation and noted that TRANSCOM already has initiated implementation of the current draft manual as a means to reevaluate identification of critical transportation assets. DOD stated that, consequently, TRANSCOM does not require additional ASD(HD&ASA) direction to do so. However, while TRANSCOM officials agreed during our review to begin reevaluating their critical assets using established criteria in the draft manual, our recommendation also calls for TRANSCOM to develop a timeline for completing this action. DOD acknowledged in its written comments that while the draft manual provides a process for critical asset identification, it has not yet provided timelines for the various milestones. DOD's comments stated that ASD(HD&ASA) will work with the various components to establish timelines, but estimated that the manual will require approximately 1 year to complete, and will require timely cooperation and participation by numerous stakeholders. We believe that establishing these timelines is essential so that TRANSCOM can reevaluate and update the identification of all critical transportation assets in a timely manner.

DOD partially concurred with our draft recommendation that TRANSCOM finalize the memorandum of understanding with the Joint Staff to discontinue the use of Transportation Infrastructure Vulnerability Assessments as its primary tool for identifying its critical assets. In its written comments, DOD noted that this recommendation contained two separate issues: (1) the discontinuation of the Transportation Infrastructure Vulnerability Assessments as means to identify critical assets and (2) the finalization of a memorandum of understanding between TRANSCOM and the Joint Staff. DOD noted in its written comments that the purpose of the memorandum of understanding is to define the roles and responsibilities of transportation subject matter experts to augment the enhanced DCIP module rather than to discontinue the use of the Transportation Infrastructure Vulnerability Assessments. In response to DOD's comments and to reflect this distinction, we made this two recommendations rather than one. DOD also stated that no additional direction on ASD(HD&ASA)'s part is required because TRANSCOM has already taken steps to address both of these issues. As noted in our report, however, TRANSCOM officials were unable to provide ASD(HD&ASA) or us with any documentation to confirm that they have discontinued the use of the Transportation Infrastructure Vulnerability Assessments. TRANSCOM's discontinuation of the Transportation Infrastructure Vulnerability Assessments as a means of identifying critical transportation assets and its adoption of the manual's methodology are both key to TRANSCOM's ability to provide DOD with an accurate list of critical

transportation assets. Further, while we recognize that TRANSCOM has taken steps to coordinate with the Joint Staff to define its roles and responsibilities for the DCIP module to the Joint Staff Integrated Vulnerability Assessment, the memorandum of understanding remains in draft. Timely completion of the draft memorandum of understanding is important so that TRANSCOM's expertise can be adequately leveraged on future vulnerability assessments of critical transportation infrastructure. Therefore, we believe this recommendation remains valid.

Finally, DOD partially concurred with our recommendation to develop and implement service-specific guidance based on published DOD DCIP guidance. In its written response, DOD stated that the Army has already developed and is implementing service-specific guidance, and it noted that the military departments prefer to wait for the official publication of the draft *DOD Critical Asset Identification Process* manual before implementing service-specific guidance. We acknowledge the Army's efforts and recognize that other military services may prefer to wait until the manual is published before they implement service-specific guidance. However, our recommendation is based on the entire body of DOD's DCIP guidance—not just the draft *DOD Critical Asset Identification Process* manual, which is focused primarily on identification of critical assets and will take at least another year to complete. In our view, service-specific DCIP guidance should be issued promptly based on DOD Directive 3020.40 and DOD Instruction 3020.45, which have been finalized at the OSD level. In the absence of timely service-specific DCIP guidance, installation personnel will continue to rely primarily on antiterrorism plans instead of on an all-hazards approach to remediate, mitigate, or otherwise reduce the vulnerabilities to critical transportation infrastructure.

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 Secretary of State; the Chairman of the Joint Chiefs of Staff; the Secretaries of the Army, the Navy, and the Air Force; the Commandant of the Marine Corps; the Combatant Commanders of the functional and geographic combatant commands; the Commander, U.S. Army Corps of Engineers; and the Director, Office of Management and Budget. We will also make copies available to others upon request.

If you or your staff have questions concerning this report, please contact me at (202) 512-5431 or 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 major contributions to this report are listed in appendix III.

Davi M. D'Agostino
Director, Defense Capabilities and
Management

Appendix I: Scope and Methodology

To conduct our review of the Department of Defense's (DOD) efforts to assure the availability of critical assets in the Transportation Defense Sector, we obtained relevant documentation and interviewed officials from the following DOD organizations:[1]

- Office of the Secretary of Defense
  - Under Secretary of Defense (Comptroller)/Chief Financial Officer
  - Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA])
- Joint Staff, Directorate for Operations, Antiterrorism and Homeland Defense
- Defense Threat Reduction Agency, Combat Support Assessments Division
- Military Services
  - Department of the Army, Asymmetric Warfare Office, Critical Infrastructure Risk Management Branch
  - Department of the Navy
    - Office of the Chief Information Officer
    - Mission Assurance Division, Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Virginia
  - Department of the Air Force, Air, Space and Information Operations, Plans, and Requirements, Homeland Defense Division
  - Headquarters, U.S. Marine Corps, Security Division, Critical Infrastructure Protection Office
- Combatant Commands
  - Headquarters, U.S. Central Command, Critical Infrastructure Program Office, MacDill Air Force Base, Florida
  - Headquarters, U.S. European Command, Critical Infrastructure Protection Program Office, Patch Barracks, Germany
  - Headquarters, U.S. Pacific Command, Antiterrorism and Critical Infrastructure Division, Camp H.M. Smith, Hawaii
    - U.S. Forces Japan
- Headquarters, U.S. Transportation Command (TRANSCOM), Critical Infrastructure Program, Scott Air Force Base, Illinois
  - Headquarters, Air Mobility Command, Homeland Defense Branch, Scott Air Force Base, Illinois
  - Headquarters, Military Sealift Command, Force Protection Office
  - Headquarters, Surface Deployment and Distribution Command, Scott Air Force Base, Illinois

[1]DOD organizations are located in the Washington, D.C., metropolitan area unless otherwise indicated.

  - Headquarters, Transportation Engineering Agency, Scott Air Force Base, Illinois
- Defense Infrastructure Sector Lead Agents
  - Headquarters, U.S. Transportation Command, Critical Infrastructure Program, Scott Air Force Base, Illinois
  - Headquarters, U.S. Army Corps of Engineers, Directorate of Military Programs
- Selected critical assets in the continental United States, Hawaii, the U.S. Territory of Guam, Germany, Greece, Kuwait and another country in U.S. Central Command's area of responsibility, and Japan

We also met with officials from the Department of Homeland Security, Infrastructure Information Collection Division, to discuss the extent to which DOD was coordinating with the Department of Homeland Security on the protection of non-DOD-owned defense critical assets in the Transportation and Public Works Defense Sectors. Further, to become more familiar with additional work being conducted on defense critical infrastructure, we met in Arlington, Virginia, with officials from the George Mason University School of Law's Critical Infrastructure Protection Program and in Washington, D.C., with the Congressional Research Service (Resources, Science, and Industry Division).

We drew a nonprobability sample of critical transportation assets located in the United States and abroad, using several critical asset lists developed by the Joint Staff, each of the four military services, and TRANSCOM. The assets we selected for review were initially drawn from the Joint Staff's list of Tier 1[2] critical transportation assets; however, the list includes only 4 Tier 1 critical transportation assets worldwide.[3] To increase the size of our

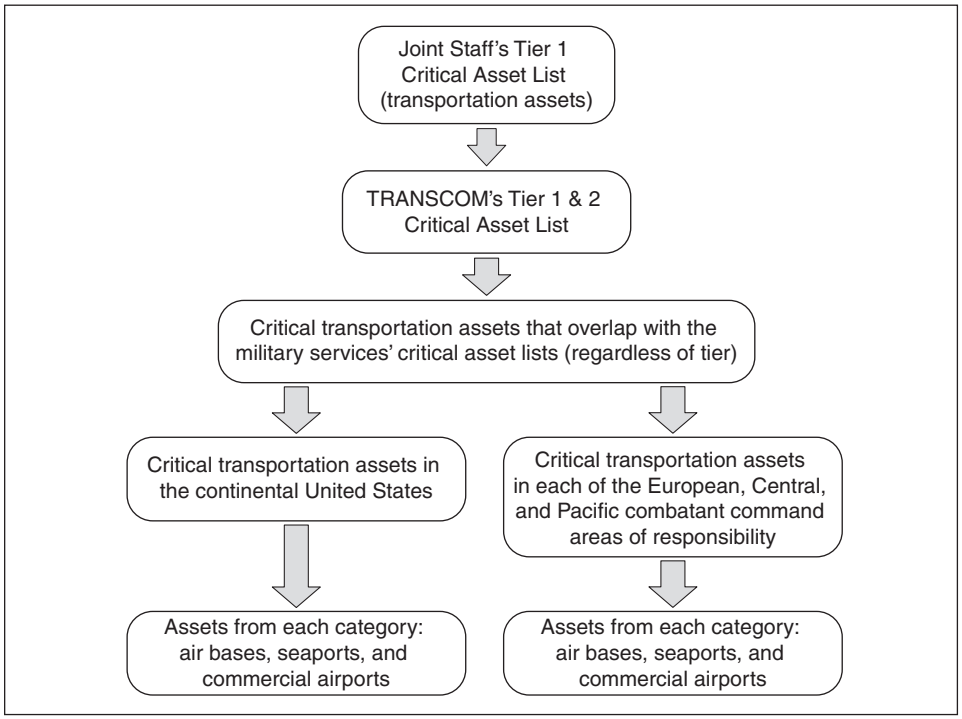
[2]Critical assets are categorized into three tiers based on their relative criticality. The loss, incapacitation, or disruption of a Tier 1 asset could result in mission (or function) failure at the DOD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level. The loss, incapacitation, or disruption of a Tier 2 asset could result in mission (or function) degradation at the DOD, military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level. The loss, incapacitation, or disruption of a Tier 3 asset could result in mission (or function) failure below the military department, combatant command, sub-unified command, defense agency, or defense infrastructure sector level.

[3]At the time of our sample selection, only four transportation assets had been identified as Tier 1 critical assets; however, TRANSCOM subsequently identified four more, raising the total to eight Tier 1 critical transportation assets. Of these assets, two were included in our sample.

sample, we used TRANSCOM's Tier 1[4] and Tier 2 critical asset lists, which together total 300 critical assets. Further, we analyzed critical asset lists from each of the four military services for overlap with TRANSCOM's critical asset list. From this, we selected 22 assets for review that included geographic dispersion among two countries in each geographic region (Europe, the Middle East, and the Pacific). We also selected assets from each military service and that were representative of the three principal types of assets identified by TRANSCOM—air base, seaport, commercial airport. Our cases for review included two of the four Tier 1 critical transportation assets. The specific assets we reviewed, their locations, and the missions that they support are omitted from this appendix, since that information is classified. Figure 6 shows the methodology we used to select the critical transportation assets for review.

[4]TRANSCOM's Tier 1 critical asset list is synonymous with the Joint Staff's Tier 1 critical transportation asset list.

Figure 6: GAO Critical Transportation Asset Selection Methodology



Source: GAO analysis of DOD data.

Table 1 shows a breakout of critical transportation assets selected by geographic combatant command.

Table 1: Number of Critical Transportation Assets Selected by Asset Category and Geographic Combatant Command Area of Responsibility

Geographic Combatant Command	Air base	Seaport	Commercial airport
U.S. Northern Command	2	1	1[a]
U.S. European Command	2[b]	0[b]	0
U.S. Central Command	2	3	1
U.S. Pacific Command[c]	4	4	2

Source: GAO analysis.

[a]Selected but not visited.

[b]One of the installations we visited in Europe identified by TRANSCOM is both an air base and a seaport.

[c]U.S. Pacific Command's area of responsibility includes Hawaii and the U.S. Territory of Guam.

Because the Joint Staff list of Tier 1 critical assets does not include critical assets from the Public Works Defense Sector, for the purposes of this report, we are treating public works assets as supporting infrastructure. For the critical transportation assets that we selected, we also spoke with the asset owners and operators about their reliance on public works assets that support the critical assets.

To evaluate TRANSCOM's identification and assessment efforts of its critical transportation assets, we reviewed documentation and guidance and met with officials from ASD(HD&ASA), the Joint Staff, the military services, and TRANSCOM. We analyzed critical asset identification criteria and guidance and compared the guidance with current asset identification efforts. In addition, we spoke with DOD installation and U.S. embassy personnel to discuss their involvement with various DOD critical asset data calls and other efforts they participated in to identify critical assets. We reviewed TRANSCOM's Transportation Infrastructure Vulnerability Assessments for assets we selected for review to determine if specific critical transportation assets below the installation level were identified. We also attempted to match these critical assets identified through the TRANSCOM's vulnerability assessments with assets listed on TRANSCOM's critical asset list.

To determine the extent to which DOD installation personnel have taken actions to help assure the availability of critical transportation assets, both within and independent of DCIP, we reviewed DOD guidance on risk management and other complementary programs. In addition, we reviewed and analyzed installation emergency management plans and continuity of operations plans to determine how, if at all, critical assets were incorporated. We also interviewed combatant command, subcomponent, and installation personnel responsible for assuring the availability of critical transportation assets to ascertain the adequacy of guidance, assessments, inspections, funding, and other processes to enhance asset availability. Finally, we assessed the supporting public works infrastructure for the 22 assets we selected for review to determine their impact on the availability of the critical asset.

To determine how DOD is funding critical transportation asset assurance, we reviewed and analyzed DCIP funding data and we interviewed officials from the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. Additionally, we interviewed officials from ASD(HD&ASA) and TRANSCOM to verify that the funding data were comprehensive and reflected DCIP funding from all sources. Further, we interviewed installation officials; personnel from U.S. Forces Japan, U.S.

European Command, U.S. Central Command, and U.S. Pacific Command; and U.S. embassy officials in Kuwait and another country in U.S. Central Command's area of responsibility, and Japan regarding other sources of funding. These sources include funding from other complementary programs or host nation contributions that provide an indirect contribution to the assurance of critical transportation assets. We found the data provided by DOD to be sufficiently reliable for representing the nature and extent of the DCIP funding.

We conducted this performance audit from May 2007 through July 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.

Appendix II: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

HOMELAND DEFENSE
& AMERICAS' SECURITY AFFAIRS

AUG 1 1 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-08-851, "Defense Critical Infrastructure: Adherence to Guidance Would Improve DoD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets," (GAO Code 351124). DoD partially concurs with the three recommendations in the report. Our response to your recommendations is enclosed.

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, (703) 602-5730, extension 143 or Antwane.Johnson@osd.mil.

Sincerely,

Paul McHale

Enclosure:
As stated

GAO DRAFT REPORT – DATED JULY 18, 2008
GAO CODE 351124/GAO-08-851

"DEFENSE CRITICAL INFRASTRUCTURE: Adherence to Guidance Would Improve DoD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense through the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD&ASA) and the Chairman of the Joint Chiefs of Staff, direct the Commander of the U.S. Transportation Command to fully implement the criteria, methodology, and process in the *DoD Critical Asset Identification Process Manual* to reevaluate and update the identification of all critical transportation assets, and develop a timeline for doing so.

DOD RESPONSE: Partially concur. ASD (HD&ASA) agrees with the recommendation to fully implement the criteria, methodology, and process in Critical Asset Identification Process (CAIP) Manual and to reevaluate and update the identification of all critical transportation assets. However, as noted in the report, the U.S. Transportation Command (USTRANSCOM) already has initiated implementation of the current draft CAIP Manual as a means to reevaluate identification of transportation-related Task Critical Assets (TCAs); consequently USTRANSCOM does not require additional ASD (HD&ASA) direction to do so.

While the draft CAIP Manual provides a process for critical asset identification, it has not yet provided timelines for the various milestones. ASD (HD&ASA) will work with Components to establish timelines. The CAIP requires close coordination between mission and asset owners, and given the complexity of interaction among the many participants in the process, we anticipate it will require approximately 1 year to complete the CAIP, and will require timely cooperation and participation by numerous stakeholders. Since the Defense Critical Asset (DCA) List is dynamic, as TCAs are identified in accordance with the Manual, they will be submitted into Strategic Mission Assurance Data System (SMADS) and may then be considered by the Joint Staff and the ASD (HD&ASA) as DCA candidates.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense through the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD&ASA) and the Chairman of the Joint Chiefs of Staff, direct the Commander of the U.S. Transportation Command to finalize the memorandum of understanding with the Joint Staff to discontinue the use of Transportation Infrastructure Vulnerability Assessments as its primary tool for identifying its critical assets.

DOD RESPONSE: Partially concur. ASD (HD&ASA) agrees with the recommendation to finalize the memorandum of understanding with the Joint Staff and to discontinue the use of

1

Transportation Infrastructure Vulnerability Assessments (TIVAs) as the primary tool to identify critical assets. However, those are two separate issues.

To accurately reflect the issues in the recommendation, request the recommendation be re-worded to read as follows: "The GAO recommends that the Secretary of Defense through the ASD (HD&ASA) and the Chairman of the Joint Chiefs of Staff, direct the Commander, U.S. Transportation Command (USTRANSCOM) to discontinue the use of TIVAs as its primary tool for identifying its critical assets and continue discussions with the Joint Staff to finalize the memorandum of understanding for USTRANSCOM CIP transportation subject matter experts to augment the enhanced DCIP module to the Joint Staff's Integrated Vulnerability Assessment when transportation assets are assessed."

As currently written, this GAO recommendation implies the purpose of the memorandum of understanding is to discontinue the execution of TIVAs. In fact, the memorandum is being developed to define the roles and responsibilities of transportation subject matter experts to augment the enhanced DCIP module. A memorandum of understanding for the discontinuance of TIVAs is not required. This discontinuance, a USTRANSCOM initiative started on June 27, 2008, has already been taken in coordination with the Joint Staff; consequently USTRANSCOM does not require additional ASD (HD&ASA) direction to do so.

As discussed in the July 1, 2008 Exit Teleconference, USTRANSCOM has already discontinued the planning and execution of its TIVAs. Assets will be identified in accordance with the Critical Asset Identification Process Manual methodology and in coordination with other Mission Owners and Resource Providers.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the Secretaries of the Military Departments to develop and implement Service-specific guidance based on published DoD Defense Critical Infrastructure Program guidance.

DOD RESPONSE: Partially concur. Although the Army has developed Service-specific guidance (AR 525-26) and HQDA Implementation Letter (in final staffing) and is executing that guidance along with DoD Directive 3020.40 and DoD Instruction 3020.45, the Military Departments prefer to await official publication of the Critical Asset Identification Process prior to implementing Service-specific guidance.

2

Appendix III: 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; Jon K. Bateman; Gina M. Flacco; James P. Krustapentus; Kate S. Lenane; Danielle Pakdaman; Terry L. Richardson; Marc J. Schwartz; John S. Townes; Cheryl A. Weissman; and Alex M. Winograd made key contributions to this report.

Related GAO Products

Defense Critical Infrastructure: Additional Air Force Actions Needed at Creech Air Force Base to Ensure Protection and Continuity of UAS Operations. GAO-08-469RNI. Washington, D.C.: April 23, 2008 (For Official Use Only).

Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets. GAO-08-373R. Washington, D.C.: April 2, 2008.

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.: August 31, 2007.

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.

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