



Highlights of [GAO-09-42](#), a report to congressional requesters

## Why GAO Did This Study

The Department of Defense (DOD) relies on a global network of DOD and non-DOD infrastructure so critical that its unavailability could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. DOD established the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure. GAO was asked to evaluate the extent to which DOD has (1) incorporated aspects of DCIP into its exercises in the Transportation Defense Sector and (2) developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise. GAO examined a nonprojectable sample of 46 critical assets representing the four military services, five combatant commands, and selected installations within five defense sectors. GAO reviewed relevant DOD DCIP guidance and documents and interviewed cognizant officials regarding DCIP exercises, training, and awareness.

## What GAO Recommends

GAO recommends that DOD (1) develop departmentwide DCIP training standards and an implementation time frame and (2) develop an effective means to communicate to installation personnel the existence and availability of DCIP expertise at the combatant command and military service levels. DOD concurred with both recommendations.

To view the full product, including the scope and methodology, click on [GAO-09-42](#). For more information, contact Davi M. D'Agostino at (202) 512-5431 or [dagostinod@gao.gov](mailto:dagostinod@gao.gov).

## DEFENSE CRITICAL INFRASTRUCTURE

### Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure

#### What GAO Found

U.S. Transportation Command (TRANSCOM) and the installations GAO visited that have critical transportation assets have incorporated aspects of critical infrastructure assurance into their exercises. DOD's DCIP guidance requires the combatant commands and the military services to conduct annual DCIP exercises, either separately or in conjunction with existing exercises. DCIP guidance also requires commanders to ensure submission of lessons learned from these exercises. For example, TRANSCOM has included aspects of critical infrastructure assurance in its two major biennial exercises. Although military personnel at 13 of the 19 installations GAO visited that have critical transportation assets generally were not aware of DCIP, GAO found that all 19 of these installations conduct routine exercises that often involve aspects of critical infrastructure assurance, and they incorporate lessons learned from past exercises into future exercises. For example, personnel at these installations conduct antiterrorism, emergency management, and continuity of operations planning exercises that often include critical assets located on the installation.

While several of the combatant commands and military services included in GAO's review of the five defense sectors have independently developed DCIP training at the headquarters level, DOD has not yet developed DCIP training standards departmentwide, and installation personnel remained largely unaware of existing DCIP expertise. DOD's DCIP instruction requires the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]) to provide policy and guidance for DCIP and oversee the implementation of DCIP education, training, and awareness of goals and objectives. ASD(HD&ASA) recognizes the need for DCIP training and program awareness, as noted in its March 2008 critical infrastructure strategy. However, given the newness of the strategy, ASD(HD&ASA) has not yet established departmentwide DCIP training standards for assuring the availability of critical infrastructure or a time frame for implementing the training standards. In the absence of established DCIP training standards, the combatant commands and military services are variously developing and implementing their own DCIP training programs. For example, the Navy has established an information assurance training program that includes a DCIP module. Furthermore, installation personnel GAO spoke with, with few exceptions, were not familiar with DCIP or aware of DCIP expertise at the combatant command and military service headquarters levels. In addition, DOD has not developed an effective way to communicate to installation personnel the existence of DCIP expertise. Consequently, they rely on other, more established programs that in some cases do not emphasize the consideration of the full spectrum of threats and hazards. Without DCIP training standards departmentwide and a means of communicating them to installation personnel, the combatant commands and military services potentially may develop mutually redundant or inconsistent training programs, and installation personnel will continue to be unaware of existing DCIP expertise.