May 2018

PROTECTING CLASSIFIED INFORMATION

Defense Security Service Should Address Challenges as New Approach Is Piloted

GAO Highlights

Highlights of GAO-18-407, a report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives

Why GAO Did This Study

Industrial security addresses the information systems, personnel, and physical security of facilities and their cleared employees who have access to or handle classified information. The National Industrial Security Program was established in 1993 to safeguard federal government classified information that may be or has been released to contractors, among others. GAO last reported on this program in 2005 and the Department of Defense has since implemented 13 of the 16 related recommendations.

GAO was asked to examine how DSS administers the program. This report assesses to what extent DSS: 1) changed how it administers the program since GAO's last report; and 2) addressed challenges as it pilots a new approach to monitoring contractors with access to classified information.

GAO reviewed guidance and regulations since 2005, including the program's operating manual. GAO analyzed data from DSS's electronic databases and also selected a non-generalizable sample of contractor facilities based on clearance level, geographic location, and type of agreement to address foreign influence. We also reviewed documents and interviewed relevant government and contractor officials.

What GAO Recommends

GAO recommends DSS determine how it will collaborate with stakeholders, including identifying roles and responsibilities and related resources, as it pilots a new approach. DSS concurred with the recommendation.

View GAO-18-407. For more information, contact Marie A. Mak at (202) 512-4841 or MakM@gao.gov.

What GAO Found

The Defense Security Service (DSS) has upgraded its capabilities but also faces challenges in administering the National Industrial Security Program, which applies to all executive branch departments and agencies, and was established to safeguard federal government classified information that current or prospective contractors may access. Since we last reported on this program in 2005, DSS has:

- streamlined facility clearance and monitoring processes, and
- strengthened the process for identifying contractors with potential foreign influence.

However, under its current approach, DSS officials indicated that they face resource constraints, such as an inability to manage workloads and complete training necessary to stay informed on current threats and technologies. In its most recent report to Congress, DSS stated that it was unable to conduct security reviews at about 60 percent of cleared facilities in fiscal year 2016. Further, DSS recently declared that the United States is facing the most significant foreign intelligence threat it has ever encountered. As a result, in 2017, DSS announced plans to transition to a new monitoring approach to address emerging threats at facilities in the program. For a comparison of the current and new approaches, see below.

Comparison of the Defense Security Service's (DSS) Current and New Approaches for Monitoring Cleared Facilities

Current Monitoring Approach	New Approach – *DSS in Transition*
Schedules security reviews on a 90-day work plan starting with specific facilities, such as those with mitigation agreements for foreign influence or classified information systems.	Will use national intelligence and Department of Defense's list of critical technologies and programs to prioritize security reviews at facilities based on their assets and the threats to those assets.
Conducts security reviews that focus on a contractor's adherence with National Industrial Security Program Operating Manual requirements.	Will conduct security reviews to develop customized security plans and assess implementation of such plans to ensure contractors protect assets.

Source: GAO analysis of DSS documentation and interviews with DSS officials. | GAO-18-407

DSS has not addressed immediate challenges that are critical to piloting this new approach. For example, GAO found it is unclear how DSS will determine what resources it needs as it has not identified roles and responsibilities. Moreover, DSS has not established how it will collaborate with stakeholders—government contracting activities, the government intelligence community, other government agencies, and contractors—under the new approach. Federal Internal Control Standards establish the importance of coordinating with stakeholders, including clearly defining roles and responsibilities. In addition, GAO's leading practices for interagency collaboration state that it is important for organizations to identify the resources necessary to accomplish objectives. Until DSS identifies roles and responsibilities and determines how it will collaborate with stakeholders for the piloting effort, it will be difficult to assess whether the new approach is effective in protecting classified information.