April 16, 2008

DEPARTMENT OF DEFENSE

Observations on the National Industrial Security Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-695T, a testimony before the House Armed Services Committee

Why GAO Did This Study

The National Industrial Security Program (NISP) aims to ensure contractors appropriately safeguard the government's classified information. NISP, along with other laws, regulations, policies, and processes, is intended to protect technologies critical to maintaining military technological superiority and other U.S. national security interests.

The Defense Security Service (DSS) within the Department of Defense (DOD) administers NISP on behalf of DOD and other federal agencies. DSS grants clearances to contractor facilities so they can access and, in some cases, store classified information. In 2005, DSS monitored over 11,000 facilities' security programs to ensure that they meet NISP requirements for protecting classified information.

In 2004 and 2005, GAO issued reports that examined DSS responsibilities related to facilities accessing or storing classified information. The first report assessed DSS oversight of facilities and DSS actions after possible compromises of classified information. The second focused specifically on DSS oversight of contractors under foreign ownership, control, or influence (FOCI). This testimony summarizes the findings of these reports and their relevance to the effective protection of technologies critical to U.S. national security interests—an area GAO designated as a governmentwide high-risk area in 2007.

To view the full product, including the scope and methodology, click on GAO-08-695T. For more information, contact Ann Calvaresi Barr at (202) 512-4841 or calvaresibarra@gao.gov.

What GAO Found

DSS did not systematically collect and analyze the information needed to assess its oversight of both contractor facilities and contractors under FOCI. While DSS maintained files on contractor facilities' security programs and their security violations, it did not use this information to determine, for example, whether certain types of violations are increasing or decreasing and why. As a result, DSS was unable to identify patterns of security violations across all facilities based on factors such as the type of work conducted, the facilities' government customer, or the facilities' corporate affiliation. Identifying such patterns would enable DSS to target needed actions to reduce the risk of classified information being compromised. With regard to contractors under FOCI, DSS did not collect and track the extent to which classified information was left in the hands of such contractors before measures were taken to reduce the risk of unauthorized foreign access. GAO found instances in which contractors did not report foreign business transactions to DSS for several months.

DSS's process for notifying government agencies of possible compromises to their classified information has also been insufficient. When a contractor facility reports a violation and the possible compromise of classified information, DSS is required to determine whether a compromise occurred and to notify the affected government agency so it can assess any damage and take actions to mitigate the effects of the suspected compromise or loss. However, for nearly 75 percent of the 93 violations GAO reviewed, DSS either made no determination regarding compromise or made a determination that was inconsistent with established criteria. In addition, in many cases in which DSS was required to notify the affected agencies of possible information compromises, the notification took more than 30 days; in one case, notification was delayed 5 months.

Despite the complexities involved in overseeing contactor facilities and contractors under FOCI, DSS field staff lacked the guidance, tools, and training necessary to effectively carry out their responsibilities. According to DSS field staff, they lacked research tools and training to fully understand, for example, the significance of corporate structures, legal ownership, and complex financial relationships when foreign entities are involved—knowledge that is needed to effectively oversee contractors under FOCI. Staff turnover and failure to implement guidance consistently also detracted from field staff's ability to effectively carry out responsibilities.

GAO has made numerous recommendations aimed at improving NISP and DSS's oversight of classified information that has been entrusted to contractors. Continued weaknesses in this and other areas that require rigorous oversight—such as export control, foreign acquisitions of U.S. companies, and foreign military sales—prompted GAO to designate the protection of critical technologies as high risk.