GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-04-332, a report to the Senate Committee on Armed Services

Why GAO Did This Study

Department of Defense (DOD) contractors perform numerous services that require access to classified information. With access comes the possibility of compromise, particularly as foreign entities increasingly seek U.S. military technologies. To ensure the protection of classified information, the National Industrial Security Program (NISP) establishes requirements that contractors must meet. In administering the NISP for DOD and 24 other government agencies, DOD's Defense Security Service (DSS) monitors whether 11,000-plus contractor facilities' security programs meet NISP requirements.

In response to a Senate report accompanying the National Defense Authorization Act for Fiscal Year 2004, GAO assessed DSS's oversight and examined DSS's actions after possible compromises of classified information.

What GAO Recommends

GAO recommends that DSS improve its oversight of contractors. GAO also recommends that DSS take steps to ensure that determinations for possible information compromises be properly made and that government agencies be quickly notified when their classified information has been lost or compromised. DOD concurred with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-332.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Katherine Schinasi at (202) 512-4841 or schinasik@gao.gov.

March 2004

INDUSTRIAL SECURITY

DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information

What GAO Found

DSS cannot provide adequate assurances to government agencies that its oversight of contractor facilities reduces the risk of information compromise. DSS is unable to provide this assurance because its performance goals and measures do not relate directly to the protection of classified information. While DSS maintains files on contractor facilities' security programs and their security violations, it does not analyze this information. Further, the manner in which this information is maintained—geographically dispersed paper-based files—does not lend itself to analysis. By not analyzing information on security violations and how well classified information is being protected across all facilities, DSS cannot identify systemic vulnerabilities and make corrective changes to reduce the risk of information compromise.

When a contractor facility reports a violation and the possible compromise of classified information, DSS does not always follow established procedures. After receiving a report of a possible information compromise, DSS is required to determine whether 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, compromise, or loss. However, DSS failed to make determinations in many of the 93 violations GAO reviewed and made inappropriate determinations in others:

- In 39 of the 93 violations, DSS made no determinations regarding compromise.
- For 30 of the remaining 54 violations, DSS's determinations were not consistent with established criteria.

As a result, government agencies are not being kept informed of possible compromises of their information.

In addition, weeks or months can pass before government agencies are notified by DSS of possible information compromises because of difficulties in identifying the affected agencies. In 11 out of 16 instances GAO reviewed, it took DSS more than 30 days to notify the affected agency that its information had been lost or compromised. DSS relies on contractor facilities to identify the affected government agencies, but some facilities cannot readily provide DSS with this information because they are subcontractors that have to obtain the identity of the government agency from the prime contractors. In one case, 5 months passed before a subcontractor facility could provide DSS with the identity of the government agency whose information was suspected of being compromised. Such delays limit the government agencies' opportunity to assess and mitigate any damage from loss or compromise.