G A O
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-706, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

June 2006

MANAGING SENSITIVE INFORMATION

DOD Can More Effectively Reduce the Risk of Classification Errors

Why GAO Did This Study

Misclassification of national security information impedes effective information sharing, can provide adversaries with information to harm the United States and its allies, and incurs millions of dollars in avoidable administrative costs. As requested, GAO examined (1) whether the implementation of the Department of Defense's (DOD) information security management program, effectively minimizes the risk of misclassification; (2) the extent to which DOD personnel follow established procedures for classifying information, to include correctly marking classified information; (3) the reliability of DOD's annual estimate of its number of classification decisions; and (4) the likelihood of DOD's meeting automatic declassification deadlines.

What GAO Recommends

To reduce the risk of misclassification and improve DOD's information security operations, GAO is recommending six actions, including several to increase program oversight and accountability. In reviewing a draft of this report, DOD concurred with GAO's recommendations. DOD also provided technical comments, which we have included as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-06-706.

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

What GAO Found

A lack of oversight and inconsistent implementation of DOD's information security program are increasing the risk of misclassification. DOD's information security program is decentralized to the DOD component level, and the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), the DOD office responsible for DOD's information security program, has limited involvement with, or oversight of, components' information security programs. While some DOD components and their subordinate commands appear to manage effective programs, GAO identified weaknesses in others in the areas of classification management training, self-inspections, and classification guides. For example, training at 9 of the 19 components and subordinate commands reviewed did not cover fundamental classification management principles, such as how to properly mark classified information or the process for determining the duration of classification. Also, OUSD(I) does not have a process to confirm whether self-inspections have been performed or to evaluate their quality. Only 8 of the 19 components performed self-inspections. GAO also found that some of the DOD components and subordinate commands that were examined routinely do not submit copies of their security classification guides, documentation that identifies which information needs protection and the reason for classification, to a central library as required. Some did not track their classification guides to ensure they were reviewed at least every 5 years for currency as required. Because of the lack of oversight and weaknesses in training, self-inspection, and security classification guide management, the Secretary of Defense cannot be assured that the information security program is effectively limiting the risk of misclassification across the department.

GAO's review of a nonprobability sample of 111 classified documents from five offices within the Office of the Secretary of Defense shows that, within these offices, DOD personnel are not uniformly following established procedures for classifying information, to include mismarking. In a document review, GAO questioned DOD officials' classification decisions for 29—that is, 26 percent of the sample. GAO also found that 92 of the 111 documents examined (83 percent) had at least one marking error, and more than half had multiple marking errors. While the results from this review cannot be generalized across DOD, they are consistent with the weaknesses GAO found in the way DOD implements its information security program.

The accuracy of DOD's classification decision estimates is questionable because of the considerable variance in how these estimates are derived across the department, and from year to year. However, beginning with the fiscal year 2005 estimates, OUSD(I) will review estimates of DOD components. This additional review could improve the accuracy of DOD's classification decision estimates if methodological inconsistencies also are reduced.