October 2006

MANAGING SENSITIVE INFORMATION

DOJ Needs a More Complete Staffing Strategy for Managing Classified Information and a Set of Internal Controls for Other Sensitive Information

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-83, a report to the Chairman, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

The September 11 attacks showed that agencies must balance the need to protect and share sensitive information to prevent future attacks. Agencies classify this information or designate it sensitive but unclassified to protect and limit access to it. The National Archives' Information Security Oversight Office (ISOO) assesses agencies' classification management programs, and in July 2004 and April 2005 recommended changes to correct problems at the Justice Department (DOJ) and Federal Bureau of Investigation (FBI). GAO was asked to examine (1) DOJ's and FBI's progress in implementing the recommendations and (2) the management controls DOJ components have to ensure the proper use of sensitive but unclassified designations. GAO reviewed ISOO's reports and agency documentation on changes implemented and controls in place, and interviewed security program managers at DOJ, its components, and ISOO to examine these issues.

What GAO Recommends

GAO recommends that DOJ assess its optimum resource needs, develop a strategy to meet them and use available resources effectively to implement all recommendations, and implement internal controls to ensure proper use of sensitive but unclassified designations. DOJ generally agreed with GAO's recommendations and provided technical comments; we included them as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-07-83.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence, (202) 512-6510, larencee@gao.gov.

What GAO Found

At the time of GAO's review, DOJ and FBI had made progress implementing ISOO's recommendations aimed at correcting deficiencies in their programs to properly classify information. FBI had taken action on 11 of 12 recommendations, including issuing security regulations governing its program and updating most of the classification guides that employees use to help them decide what information should be classified. FBI is also correcting deficiencies in its training and oversight activities. If FBI completes all recommendations, this will help to lower program risk since it makes 98 percent of DOJ's classification decisions. DOJ had taken action on 5 of 10 recommendations, including fixing problems with outdated and insufficient training and insufficient monitoring of components' programs. DOJ, however, has taken no action on the most important recommendation, addressing its staff shortages, which continue to place its program at risk given that it sets policy, provides training, and oversees classification practices departmentwide. DOJ said it did not have staff resources to address other shortcomings in its training and oversight activities that ISOO recommended it correct. DOJ is trying to address its resource constraints, a long-standing problem that GAO identified as early as 1993, by requesting additional funds from an administrative account in fiscal year 2007. However, DOJ does not know the optimum number of staff it needs for the program because it has not assessed its needs. It also does not have a strategy that identifies how it will use additional resources to address remaining deficiencies so as to reduce the highest program risks, such as whether to first address training, oversight, or other program gaps.

For sensitive but unclassified information, the five components in our review —Bureau of Alcohol, Tobacco, Firearms and Explosives; Criminal Division; Drug Enforcement Administration; FBI; and U.S. Marshals Service—had orders and directives that identified and defined the various designations components were using, such as Law Enforcement Sensitive, to protect information, such as information critical to a criminal prosecution. But the components did not have specific guides, with examples, to help employees decide whether information merits a sensitive but unclassified designation. Furthermore, none of the components had training to help employees make these decisions or oversight of their designation practices. Without these controls, DOJ cannot reasonably ensure that information is properly restricted or disclosed and that designations are consistently applied. GAO recently identified similar problems at several other agencies and recommended that they implement such controls, and the agencies agreed to do so. According to security officials, DOJ is waiting for the results of an interagency working group established to set governmentwide standards for sensitive but unclassified information before considering additional changes in its sensitive but unclassified practices or those of its components. The final results from the working group are due by the end of December 2006. Once standardization is realized, it is important for DOJ to ensure that sensitive but unclassified practices across the agency provide employees with the tools they need to apply designations appropriately.