United States Government Accountability Office

GAO

Report to the Chairman, Committee on the Judiciary, House of Representatives

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-07-83

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.

Contents

Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
DEA	Drug Enforcement Administration
DEA-S	DEA-Sensitive
DOJ	Department of Justice
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GSA	General Services Administration
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
LES	Law Enforcement Sensitive
LOU	Limited Official Use
PROPIN	Proprietary Information
SEPS	Security and Emergency Planning Staff
USMS	U.S. Marshals Service

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 20, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

According to the former Vice Chair of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the government's single greatest failure in the lead-up to the September 11, 2001, attacks was the inability of federal agencies to share information about suspected terrorists and their activities. Likewise, as we have previously reported, critical to homeland protection efforts is the ability to share information among key homeland security stakeholders so they can coordinate their antiterrorism activities yet also protect sensitive information from unauthorized access that could compromise our nation's security.[1] As part of these protection efforts, pursuant to Executive Order 12958, as amended, the federal government routinely classifies certain documents and other information critical to our national security as Top Secret, Secret, or Confidential.[2] These classification levels indicate the degree of damage that could be reasonably expected from unauthorized disclosure. Classified information can only be used by individuals who have an appropriate security clearance and a need to know and must be safeguarded from unauthorized access and disclosure. A critical component of balancing the competing interests of the need to share and the need to protect information is the establishment of clear policies and procedures to guide decisions on whether information should be classified.

Reviewing classified information to determine if it must continue to be restricted or if it can be declassified and be made publicly available and shared is also a vital part of the classification system. For example, under

[1] GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[2] See Exec. Order No. 13292, 68 Fed. Reg. 15,315 (Mar. 28, 2003). See also 32 C.F.R. pt. 2001.

a provision in the executive order, all records of a permanent historical value over 25 years old that contain classified national security information will be automatically declassified on December 31, 2006, and each year thereafter, and may be available for public disclosure.[3] Before this date, agencies may review applicable records to determine if they qualify for certain exemptions—for example, information about the confidential human sources of intelligence information cannot be disclosed—if they should be reclassified, or if they should be withheld for reasons such as concerns about an individual's privacy rights.

Government agencies may also designate other types of information important to their missions, such as law enforcement information critical to a prosecution, as sensitive but unclassified. Agencies have employed a number of different sensitive but unclassified designations, such as Law Enforcement Sensitive, For Official Use Only, and Limited Official Use, which have associated restrictions on handling and sharing such information with other government entities and with the public. Sensitive but unclassified information generally must be safeguarded from public release and can only be used by those with a need to know. Unlike classified information, generally, a security clearance is not required for access to sensitive but unclassified information, and there is no time limit on the designation indicating when it can be removed.

As part of the post-September 11 efforts to better share information critical to homeland protection, agencies' classification and sensitive but unclassified information security programs have come under scrutiny. In response to congressional requests, we have recently published several reports assessing various executive branch agencies' programs for designating and sharing classified and sensitive but unclassified information. (See app. I for summaries of each of our related reports.) This work noted that agencies needed to enhance their policies and procedures governing classified and other sensitive information to help ensure they were appropriately protecting it. For example, we found that the Department of Defense's information security program had weaknesses, such as in the training provided employees on the classification program, and in the use of self-inspections to monitor program implementation.[4] In

[3] Declassified information may continue to be withheld from public disclosure for reasons under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, or other legal authority, or may be reclassified in accordance with the executive order.

[4] GAO, *Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors*, GAO-06-706 (Washington, D.C.: June 30, 2006).

addition, congressional committees have conducted a number of hearings on agencies' information security efforts that raised issues such as whether some agencies have been overclassifying documents, thereby restricting public access to important historical information.

The Information Security Oversight Office (ISOO), an office within the National Archives and Records Administration, is responsible for issuing directives to implement the executive order that governs classified information. The office is also responsible for overseeing executive branch agencies' national security information classification programs for compliance with the order and implementing directives.[5] The office is not responsible for overseeing agencies' sensitive but unclassified information security programs, which is the responsibility of each agency. ISOO's oversight consists of performing on-site inspections of classification programs, conducting classified document reviews, evaluating agency security education and training programs, and recommending corrective actions to agencies when it finds violations under the order or directives. According to ISOO, while the order provides it with the authority to make such recommendations, it cannot require agencies to implement them.[6] ISOO is also required to report at least annually to the President on the status of federal agencies' national security information classification programs.

The Department of Justice (DOJ), the nation's top law enforcement agency, is the third largest classifier of information in the executive branch, following the Department of Defense and the Central Intelligence Agency, based on information that these agencies reported to ISOO. Furthermore, one component within DOJ, the Federal Bureau of Investigation (FBI), makes up 98 percent of the department's total classification decisions. Thus, it is important that both organizations have effective information classification programs. In July 2004, ISOO made 10 recommendations to DOJ to correct deficiencies in its policies and procedures for classifying and declassifying national security information. For example, ISOO found gaps in the level of resources DOJ had available to oversee its classification management program, in its employee training programs, and in the use of inspections to ensure employees were making proper classification decisions. In response, ISOO recommended that DOJ

[5] See 32 C.F.R. pt. 2001.

[6] The executive order does, however, authorize the imposition of sanctions in the event of a knowing, willful, or negligent violation of the order or its implementing directives.

provide more resources, update and more consistently provide employee training, and conduct more regular inspections of how well its classification management program is working to correct these deficiencies. Likewise, ISOO made 12 recommendations to the FBI in April 2005 to address deficiencies in that component's program, including gaps in the guidance employees can use to make classification decisions, outdated training, and little program oversight. ISOO recommended that the FBI issue regulations governing the program, update or create classification and declassification guides to help employees properly classify information, update employee training, and use more regular inspections to test program effectiveness.

In response to your request, this report examines matters related to DOJ's management of classified and sensitive but unclassified information. More specifically, we address the following questions:

1. To what extent has DOJ implemented ISOO's recommendations?

2. To what extent has FBI implemented ISOO's recommendations?

3. What policies, procedures, and internal controls are in place in selected DOJ components to properly use sensitive but unclassified designations?

4. What processes are in place at selected DOJ components to respond to intragovernmental requests to share national security and sensitive but unclassified information?

To determine the extent of changes that DOJ and the FBI have made to implement ISOO's recommendations and other changes made to improve their classification management programs, we (1) reviewed the results of ISOO's audits; (2) obtained supporting documents that addressed these changes, when available; and (3) discussed challenges that DOJ and FBI managers responsible for implementing and overseeing these programs faced in making these changes. While these results cannot be generalized to all classified documents, we determined the methodology ISOO uses to conduct its reviews is adequate to support its recommendations.

To determine the extent of policies, procedures, and internal controls that selected DOJ components have in place for designating information as sensitive but unclassified, we used our *Standards for Internal Control in*

the Federal Government to provide criteria to assess the components' sensitive but unclassified designation practices.[7] We selected five DOJ components for our review: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Criminal Division; Drug Enforcement Administration (DEA); the FBI; and U.S. Marshals Service (USMS). We selected these components because, on the basis of data we collected as part of our prior governmentwide assessment of 26 agencies' sensitive but unclassified information programs, we determined that each of these components had adopted one or more sensitive but unclassified designations, in addition to the Limited Official Use designation used across the department.[8] We reviewed the available data collected on these five components as part of the governmentwide review. We had determined these data were reliable enough for our purposes, and we conducted follow-up interviews with each component's security officials and senior program officials on these issues.

To determine how selected DOJ components respond to federal intragovernmental requests for classified and sensitive but unclassified information, we reviewed supporting documents when available, interviewed these same security officials, and compared the components' processes for responding to requests, but we did not independently test the effectiveness of these processes. We conducted our work from June 2005 through August 2006 in accordance with generally accepted government auditing standards. More detailed information about our scope and methodology appears in appendix II.

Results in Brief

At the time of our review, though DOJ had fully or partially implemented 5 of ISOO's 10 recommendations made in 2004 to correct deficiencies in the department's classification management program, the department's program remains at risk because DOJ has not addressed the need for more staff, and this need in turn hinders the department's ability to address remaining ISOO recommendations and to provide training and oversight of classification practices across the department and its components.

[7] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[8] That review covered 26 agencies, 24 of which are subject to the Chief Financial Officers Act. The other two, the Federal Energy Regulatory Commission and the U.S. Postal Service, were included because our previous experience indicated that they used sensitive but unclassified designations.

Specifically, DOJ fully completed action requiring regular program inspection reports from its components and partially implemented four other recommendations, including updating classification management training and taking action to ensure that all security program managers who handle classified information have security clearances. However, DOJ disagreed with the recommendation to elevate the position of its security office within the department, stating that the program managers of that office already had adequate access to senior leadership. Nevertheless, ISOO still maintains this change is needed. The department has not addressed other recommendations that pertained to ensuring that all employees leaving the agency are briefed on the continued need to protect classified information, following up on problems identified from inspections, and monitoring employees' classification practices. Moreover, the department has not addressed the important issue of insufficient staff resources to effectively manage and oversee its program. DOJ had one staff to cover departmentwide training issues and three staff to oversee 3,500 locations under the program. According to the program manager, with these resources, the security office was reacting to classification issues that arose rather than being proactive to prevent them. DOJ has not corrected its resource gap, a problem we also identified in 1993,[9] because the department's security office did not receive additional resources, as requested, nor has DOJ reallocated resources from other activities to that office, according to DOJ security officials, although the department would not provide additional information on the reasons more funding was not made available. The security office has asked the governing board of its Working Capital Fund—an administrative fund that recovers operating costs by charging components fees for certain services the department provides them—for fiscal year 2007 funds to provide 9 more staff for the program, for a total of 22. But the program manager is uncertain whether even these resources will be sufficient for an effective program, in part because the security office has not assessed its optimum staffing levels. In addition, the office does not have a strategy that lays out how it will divide these resources to address the remaining deficiencies ISOO identified in ways that reduce the most risks to protecting national security information, such as whether to focus on addressing training, oversight, or other program gaps first. In providing technical comments on a draft of the report, DOJ acknowledged that it has not conducted a formal assessment of the optimal level of resources its security office needs to administer the

[9] GAO, *Document Security: Justice Can Improve Its Controls Over Classified and Sensitive Documents*, GAO/GGD-93-134 (Washington, D.C.: Sept. 7, 1993).

information security program. DOJ also stated that its security office identified in budget documents how these resources would be allocated to address the remaining deficiencies identified by ISOO. However, DOJ provided no evidence of its security office's strategy for allocating the 9 additional staff. Our previous work has identified the importance of conducting a workforce analysis and developing a strategy to fill identified staffing gaps, both of which are characteristic of best practices followed by high-performing organizations.[10]

The FBI had begun or completed actions in response to all but one of the 12 recommendations that ISOO made in its April 2005 report for correcting deficiencies in the FBI's classification management program guidance, training, and oversight. If FBI completes all recommendations, this will help to lower program risk since it makes 98 percent of the classification decisions at DOJ. At the time of our review, the FBI had issued security regulations on both its classification management program and its method of processing program violations, as well as instituted certain program inspection practices. The FBI had also updated most of its guides to employees on how to classify information and developed a guide on how to declassify it—actions ISOO cited as key to helping ensure employees have current, clear, and consistent guidance to make decisions on what information to protect and restrict and what information to release and share. Issuance of its revised primary classification guide was pending at the time of our review because the agency was awaiting resolution of some outstanding intelligence-related issues that would affect the guide's content. Likewise, issuance of its declassification guide was pending because the agency was responding to comments on the draft from the Interagency Security Classification Appeals Panel with purview over the guide.[11] Finally, the FBI disagreed with the need to develop a system that imposes graduated and significant sanctions for serious classification management violations committed by repeat offenders, asserting the agency had penalty provisions in place that achieved this outcome. Upon review of aspects of the sanctions system FBI has in place, ISOO officials agreed that the system responds to this recommendation.

[10] GAO, *Human Capital: Implementing an Effective Workforce Strategy Would Help EPA to Achieve Its Strategic Goals*, GAO-01-812 (Washington, D.C.: July 31, 2001).

[11] The Interagency Security Classification Appeals Panel approves, denies, or amends agency exemptions from automatic declassification. It also decides on appeals by persons who have filed classification challenges and appeals by persons or entities who have filed requests for a mandatory declassification review.

For sensitive but unclassified information, the five components we reviewed had orders and directives in place to identify the various types of categories they used and to describe how information should be handled and protected. However, none of these components had specific guidance, training, and oversight in place to help ensure employees properly designate information as sensitive—for example, information shared with law enforcement agencies to support their criminal investigations or anti-terrorism activities—and to therefore protect it from unauthorized access. Without these internal controls, information essential to homeland protection may be unduly restricted or improperly disclosed. The orders and directives that components issued do not provide employees with specific guidance on how to decide whether information should be designated in this way. For example, manuals developed by the FBI and Drug Enforcement Administration define the terms "Law Enforcement Sensitive" and "For Official Use Only," but do not provide criteria and examples employees can use to decide if information merits these designations. We also recognized the need for such guidance in our governmentwide assessment of agencies' designation practices and recommended that the Office of Management and Budget ensure agencies have this key internal control in place.[12] This is particularly important for DOJ, since its components use a variety of designations, such as Law Enforcement Sensitive and DEA-Sensitive, that may be difficult to distinguish. According to DOJ program officials, the department is not revising its guidance now because it is waiting for the results of an interagency working group—due by the end of December 2006—that was created in response to a December 2005 presidential memorandum to standardize designations across the government. We also found that none of the components provide employees with formal training on using designations or oversee how their designation practices are working. These gaps are particularly of concern in three of the components that do not restrict the number of employees who can make designation decisions and yet do not provide them guidance and training on how to make them. We recently made recommendations to the Departments of Energy[13] and Homeland Security[14] to correct similar deficiencies in their designation

[12] GAO-06-385.

[13] GAO, *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved*, GAO-06-369 (Washington, D.C.: Mar. 7, 2006).

[14] GAO, *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO-05-677 (Washington, D.C.: June 29, 2005).

practices, and the agencies have agreed to improve their program guidance, training, and oversight.

All of the components in our review reported having processes for responding to intragovernmental requests for national security or sensitive but unclassified information from Congress, executive agencies, and other federal sources, and we found that the processes are consistent with federal internal control standards. For example, the components reported having specified clear lines of authority and responsibility for responding to intragovernmental requests. According to agency officials in the components, these inquiries come through central offices and are to be forwarded to subject matter experts with the relevant knowledge to determine whether information can be disseminated. These experts use consultation with other knowledgeable agency personnel, such as their general counsels; professional judgment on the nature and sensitivity of the information; and any available policies and procedures when considering how to respond to requests. In addition, a unit supervisor—such as a Section Chief—is to review the response before it is released to the requester. Finally, all of the components reported communicating with requesters at various points during the response process to, for instance, clarify their requests or explain why information cannot be released.

We are recommending that the Attorney General determine the staff resource level required for carrying out the responsibilities of the department's classification management program, including full implementation of ISOO's recommendations, and devise a strategy to make resources available and use them most effectively. For sensitive but unclassified information, we are recommending that the Attorney General ensure that DOJ components have internal controls in place—namely, specific guidance, training, and oversight—once the interagency working group has completed its efforts.

Background

The U.S. government classifies information that it determines could reasonably be expected to damage the national security of the United States if disclosed publicly. Since 1940, the classification of official secrets has been governed by policies and procedures flowing from executive orders issued by presidents, largely based on authority granted under Article II of the Constitution. Current classification and declassification requirements are mandated by Executive Order 12958, *Classified National*

Security Information, as amended.[15] The order establishes the basis for classifying national security information at one of three levels—Top Secret, Secret, or Confidential—depending on the degree of damage that unauthorized disclosure of this information could reasonably be expected to cause to the national security of the United States.[16] Pursuant to the executive order, designated individuals, called original classifiers, exercise original classification authority, meaning they can classify national security information for the first time. Such individuals, including the President, agency heads, and other government officials that have been delegated this authority determine the degree of damage that disclosure could cause, decide on a classification level for the information, and attempt to establish a date or event for its declassification.

Declassification is a vital part of the classification system because it prompts the change in status of the information from classified to unclassified, which may make it available for others to access and use, such as members of the general public, researchers, historians, or other parties. Under the automatic declassification provision of the executive order, all records of a permanent historical value over 25 years old that contain classified national security information will be automatically declassified on December 31, 2006, and each year thereafter, and may be available for public disclosure, unless an agency head or senior agency official determines that these records fall within an exemption that permits continued classification as approved by the President or the Interagency Security Classification Appeals Panel.[17] Examples of exemptions include information that, if released, could be expected to seriously impair relations between the United States and a foreign government; undermine diplomatic activities of the United States; identify a human intelligence source; or violate a statute, treaty, or international agreement. Information that is automatically declassified as of December 31, 2006, will not necessarily enter the public domain. According to ISOO

[15] See Exec. Order No. 13292, 68 Fed. Reg. 15,315 (Mar. 28, 2003). See also 32 C.F.R. pt. 2001.

[16] The executive order describes the degree of damage to the United States that unauthorized disclosure of national security information reasonably could be expected to cause as exceptionally grave damage, serious damage, or damage and the corresponding levels for classifying this information as Top Secret, Secret, or Confidential, respectively. The order also defines national security as national defense or foreign relations of the United States.

[17] Pursuant to section 3.3 of the executive order, automatic declassification will occur whether or not the records have been reviewed.

officials, declassified information may continue to be withheld from public disclosure for reasons under the Freedom of Information Act (FOIA) or other legal authority or may be reclassified in accordance with the executive order.[18]

The order also requires ISOO to implement directives and perform oversight inspections of executive branch agencies' national security information classification programs to ensure these programs are in compliance with the order. When the oversight inspections result in findings of noncompliance with the order, ISOO recommends corrective actions to the agencies. However, according to ISOO, it cannot require agencies to implement the recommended corrective actions.

According to ISOO, DOJ is the third largest classifier of information in the executive branch, although this represents about 2 percent of all executive branch classification decisions during fiscal years 2000 through 2004, as the vast majority of classified information originates in the Department of Defense. Nevertheless, DOJ is responsible for a large volume of classified information, some of which if improperly disclosed could harm the national security of the United States. The majority (approximately 98 percent) of classification activity within DOJ occurs at the FBI.

DOJ also designates certain information as sensitive but unclassified and prescribes specific requirements for handling and sharing this information to ensure that harm is not caused to governmental, commercial, or privacy interests as a result of disclosing it to the public or persons who do not need such information to perform their jobs. DOJ components in our review use a number of sensitive but unclassified designations, such as Law Enforcement Sensitive, For Official Use Only, and Limited Official Use, to identify information as sensitive but unclassified. Such information at DOJ could include that which is critical to a criminal prosecution. As such, the department would protect this information from inappropriate dissemination by designating it Law Enforcement Sensitive and applying prescribed dissemination and handling procedures that correspond with the designation. Information designated as sensitive but unclassified remains so indefinitely, unless it is reviewed, for example, pursuant to a request under FOIA. That act requires federal agencies to disclose records requested in writing by any person unless one or more of the nine exemptions and three exclusions authorize the agency to withhold the

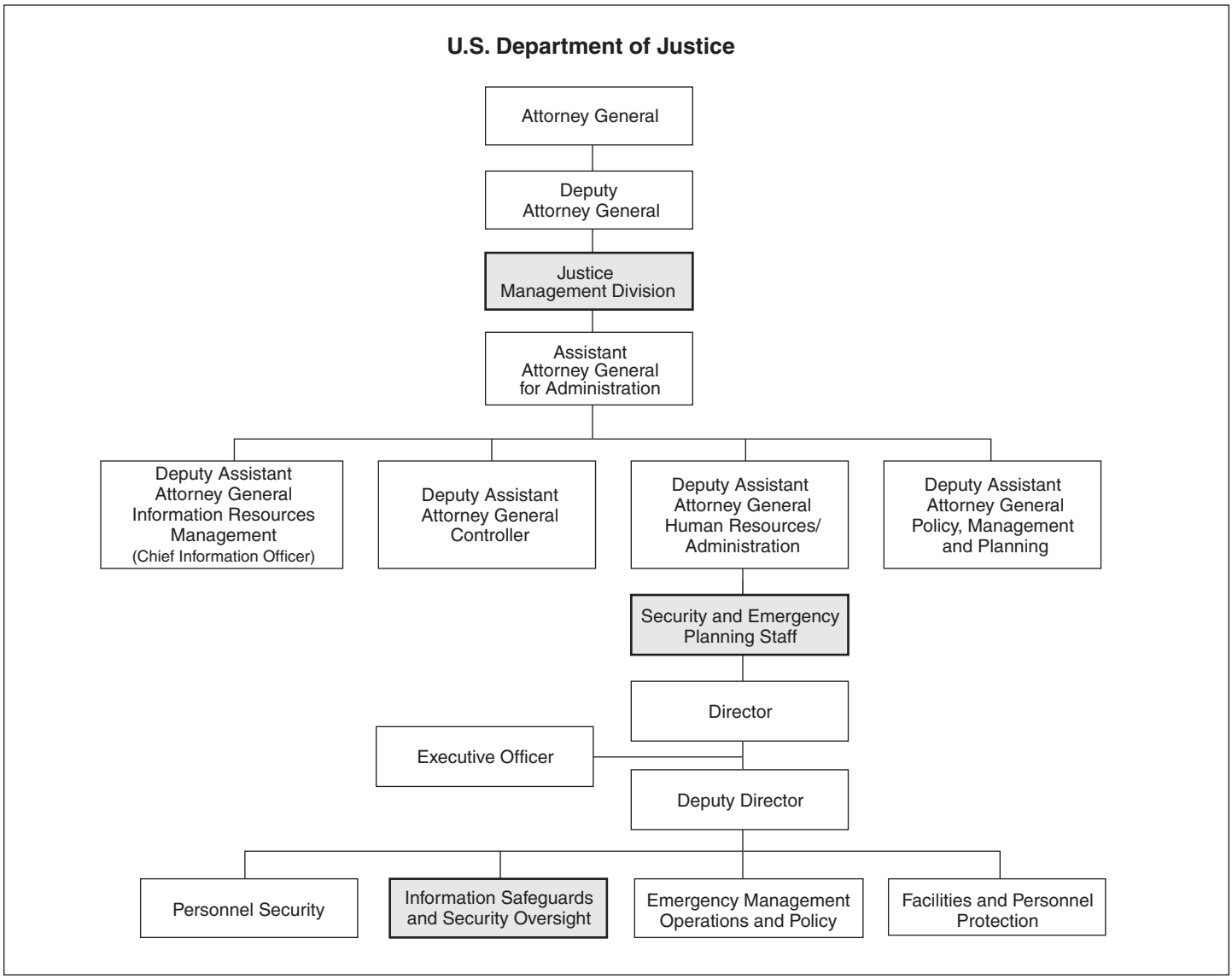
[18] See, e.g., 5 U.S.C. § 552.

requested information. For example, law enforcement records may be withheld if their release could reasonably be expected to interfere with enforcement proceedings.

Within DOJ, the Office of Information Safeguards and Security Oversight, which is part of the Security and Emergency Planning Staff (SEPS), is responsible for developing security policy and administering and overseeing the department's programs for managing classified and sensitive but unclassified information. This office currently has a total of 13 staff, of which 1 is responsible for policy development and training, and 3 are responsible for program oversight. The remaining 9, among other things, administer the department's sensitive compartmented information program,[19] reviews information technology security policies developed by the department's Chief Information Officer, and ensures the development and implementation of departmentwide policies and procedures that govern certain security related activities. Figure 1 shows an excerpt of DOJ's organizational chart that features the offices responsible for classification management.

[19] Sensitive compartmented information is classified information concerning or derived from intelligence sources, methods, or analytical processes. This information is required to be handled within formal access control systems established by the Director of the Central Intelligence Agency.

Figure 1: DOJ Organizational Chart



Source: Developed by GAO based on DOJ data.

At the component level, security program managers are responsible for implementing component-specific security activities, such as conducting internal inspections and training employees on their responsibilities in relation to DOJ's security programs. In total, there are approximately 40 security program managers and alternates, 33 of which conduct these duties on a part-time basis.

DOJ shares classified and sensitive but unclassified information with those who have a need to know this information, such as with other law enforcement agencies at all levels of government. One manner in which DOJ shares this information is in response to requests it receives from other federal entities, such as Congress, other executive agencies, and legislative agencies.

DOJ Has Made Progress Implementing ISOO Recommendations but Has Not Yet Addressed Critical Staff Resource Issues That Limit Its Ability to Address All Needed Changes

Although DOJ has completed or partially completed half of ISOO's 10 recommendations, it has not implemented the other half, primarily because of resource constraints, according to DOJ. This has been a long-standing problem in the program, as our prior work shows, but DOJ reported that it is seeking additional resources from an administrative fund in fiscal year 2007. The ISOO recommendations were to correct, among other things, resource constraints, a lack of sufficient training on how to classify information, and inadequate oversight to ensure its classification management practices were working well. DOJ is not certain that the additional resources will be enough for an effective program. However, it has not assessed the optimum resources it needs or developed a strategy to use available resources most effectively to resolve remaining deficiencies.

DOJ Took Action on 5 of the 10 ISOO Recommendations for Its Classification Management Program

ISOO made 10 recommendations to DOJ in July 2004 aimed at resolving deficiencies in DOJ's classification management program, and, at the time of our review, the department had completed or partially addressed half of the recommendations, as table 1 shows.

Table 1: Status of DOJ's Implementation of ISOO's Recommendations as of August 2006

ISOO's recommendations to DOJ	
	Fully implemented
1.	Consider requiring components to file self-inspection reports of their security classification programs as a matter of course, not just when there are significant findings.
	Partially implemented
2.	Require all security program managers to hold security clearances at the level appropriate for the activity of their offices, including managing classified information.
3.	Take steps to ensure required refresher training is received by everyone in all components and that this training includes how to properly decide to classify and mark information.
4.	Ensure all security program managers receive regular and consistent training on classification practices.
5.	Take steps to properly track security violations, including handling classified information, throughout the department, analyze the violations for trends, and incorporate the findings into its security education and training program.
	Not implemented
6.	Commit sufficient resources to effectively implement its departmental classification management and security program as called for in Executive Order 12958, as amended.
7.	Enforce the requirement that staff, when they terminate employment, be briefed on their continued information security responsibilities.
8.	Develop a follow up mechanism to ensure security program managers perform annual internal inspections of classification management and security programs as required by DOJ's *Security Program Operating Manual*.
9.	Review classified documents, after DOJ staff have received training on marking requirements, to determine if staff are properly applying the required markings, and review classified documents on a regular basis, such as during annual and recurring inspections, to ensure proper classification decisions and practices.
	Disagreed with recommended change
10.	Examine the placement of DOJ's departmental security office—Security and Emergency Planning Staff—within the department's organizational structure and consider repositioning it to afford it higher visibility and increased stature in the implementation of the classified information security program at DOJ.

Source: GAO analysis of DOJ information.

Through SEPS, DOJ had implemented 1 recommendation to require that each of its components file self-inspection reports on its classification management program as a matter of course by including this requirement in its May 2005 revised *Security Program Operating Manual*. DOJ also built in the requirement that all components submit inspection reports for each fiscal year no later than October 15 of the following fiscal year, but at

the time of our review, a SEPS official noted that none of the components had submitted inspection reports for fiscal year 2005.

Through SEPS, DOJ has partially implemented 2 other recommendations. First, in response to ISOO's recommendation that security program managers hold security clearances at levels appropriate for the activity of their office, SEPS reported that all of its component security program managers who handle classified information had security clearances, but SEPS was considering revising the order on security programs and responsibilities to include a requirement for these managers to hold clearances. Second, as of April 2006, SEPS reported that it has taken steps to make refresher training, including how to mark classified documents, available to all staff in all DOJ components. According to DOJ security officials, SEPS has developed a computer-based refresher training module, which is estimated to be available to employees by December 2006.

DOJ disagreed with an ISOO recommendation to examine the placement of SEPS within the department's organizational structure and consider repositioning it to afford it higher visibility and increased stature. DOJ's Assistant Attorney General for Administration informed ISOO that SEPS's reporting to the Deputy Assistant Attorney General for Administration does not hinder it from fulfilling its responsibilities, and SEPS's director has access to the department's senior leadership whenever needed. However, ISOO still maintains this change is needed.

DOJ's Inaction on Staff Resource Issues Impedes Full Implementation of ISOO's Recommendations

ISOO reported that SEPS lacked sufficient staff resources to effectively implement DOJ's classification management program and recommended that measures be taken to correct this deficiency. ISOO's recommendation to DOJ on resources for classification management is consistent with the executive order governing classified information that requires agency heads to commit the resources necessary to effectively implement a national security information program. The order also requires the senior agency official—who is designated by the agency head to direct and administer the agency's classified national security information program—in part, to establish and maintain programs to (1) train and educate employees on the need to properly classify and mark national security information and prevent unnecessary access to and unauthorized disclosure of classified information; and (2) provide oversight of the program through mechanisms such as ongoing internal inspections. These requirements are also consistent with federal standards for internal control.

ISOO reported that SEPS's lack of resources is particularly significant because of DOJ's large volume of classification activity—especially when SEPS is compared to security offices at other federal agencies of similar size and structure. DOJ, the third largest classifier of information in the federal government, has 13 full-time positions devoted to information security. Four of the 13 are dedicated to DOJ's classification management training and program oversight departmentwide, 1 to provide and oversee training across the department and components and 3 to conduct security compliance reviews at DOJ's 3,500 locations. DOJ does have security program managers at each of its components to provide training and program oversight for that component that helps to supplement departmental activity. Nevertheless, in comparison, the Department of Energy, the fifth largest classifier, has 23 full-time positions, and the Department of State, the fourth largest classifier of information, has 8 full-time positions to cover its classification management program at headquarters alone, according to ISOO.

SEPS did not receive additional resources, as requested, nor did DOJ reallocate resources to SEPS from other activities, according to DOJ security officials, although they would not provide additional information explaining the reasons why funds were not made available. This problem is longstanding. In 1993, for example, we reported that limited staff resources in SEPS's Security Compliance Review Group affected its ability to conduct compliance reviews of all DOJ locations in overseeing the department's security program.[20] In addition, during 1991 and 1992, the group had 6 employees to conduct reviews of 1,300 DOJ locations compared to half as many staff to cover almost three times as many locations today. Moreover, in 1993, we reported that DOJ requested, but was not authorized, additional staff, and we recommended that the Attorney General direct SEPS's Security Compliance Review Group to explore other alternatives for selecting and conducting these annual reviews to maximize the use of its limited resources. In response, DOJ devised a strategy to use components' security specialists to help with compliance reviews and their inspection reports to target locations to review. As a result, DOJ reported that the number of compliance, follow-up, and unscheduled reviews increased. However, at the time of our review, SEPS indicated that security program officials only perform oversight of their components' security programs. Despite the progress reported after our 1993 report, ISOO found over 10 years later that DOJ

[20] GAO/GGD-93-134.

was not able to compensate for its lack of resources and provide sufficient oversight.

As a result of these staff resource limitations, DOJ security officials stated that SEPS had only been able to partially implement 2 ISOO recommendations and had not taken steps to address 3 others. DOJ had partially responded to ISOO's recommendation that department security program managers be given consistent and regular training they need to understand their responsibilities for managing their respective component's classification activities. SEPS agreed to provide training to these managers in two ways: (1) an annual conference, at which attendance is not required, that the department has hosted since 2003 and (2) detailed training workshops on handling and safeguarding classified information, such as marking documents, conducting self-inspections, and managing classification programs, which are provided only upon request. However, DOJ does not have a mechanism, as called for in our federal internal control standards, and sufficient staff, as ISOO noted in its report, to ensure all security program managers consistently receive the training they need. In addition, SEPS has implemented a database to track security incidents departmentwide, such as classification program violations, as ISOO recommended. However, SEPS officials reported that they have not been able to monitor security violations and incidents to identify patterns and trends and incorporate these lessons learned into the department's security education and training program because they lack the staff to do so.

The three recommendations SEPS had not taken any action on primarily related to monitoring aspects of the classification management program. First, ISOO found that SEPS was not conducting frequent reviews of the department's compliance with the security program, as a whole, and that the components were not supplementing these department-level reviews by conducting self-inspections of compliance with their security programs on a frequent and consistent basis to ensure that sound security practices are maintained. SEPS's team of three reviewers was responsible for conducting security program compliance reviews at an estimated 3,500 DOJ facilities currently located worldwide. ISOO also found that SEPS had not established a mechanism to ensure that components were conducting the self-inspections. ISOO recommended that DOJ correct these deficiencies.

Second, ISOO also found that classified documents were not always marked as required. Over half of the 81 classified documents that ISOO reviewed did not meet the marking requirements of the executive order.

The most frequent marking errors consisted of a lack of, or incomplete, portion markings (27 documents) and missing, incomplete, or improper declassification instructions (23 documents). Therefore, ISOO recommended that DOJ review classified documents on a regular basis to determine if staff are properly applying the marking requirements after employees have been trained on these requirements. According to SEPS officials, because of related resource constraints, the office had not taken action to institute these reviews.

Third, DOJ had not taken action on ISOO's recommendation that employees receive security debriefings upon leaving the department. ISOO reported that such termination briefings are essential to informing employees that were leaving the agency of their continuing responsibility to protect classified security information. This recommendation is consistent with the executive order and implementing directives, federal standards for internal control, and DOJ's own *Security Program Operating Manual*. DOJ reported that it enforces this requirement by checking to see if components are providing the briefings when SEPS conducts components' security compliance reviews. However, ISOO found that SEPS did not conduct these reviews frequently enough to ensure that sound security practices are maintained. Furthermore, DOJ officials concurred with ISOO's position on this matter and attributed the department's insufficient reviews to its resource limitations. As an alternative, ISOO suggested to us that DOJ might coordinate with its human resources department to establish a system to track whether employees received the termination briefings before departure.

To address its resource constraints, SEPS expects to add 9 more staff—5 full-time employees and 4 contract employees—to the 13 it currently has on board, pending the department's Customer Advisory Board approval of funds from its Working Capital Fund. This fund is an administrative account generally intended to recover operating costs by having the department charge components fees for common administrative services—such as financial, telecommunications, and personnel services—

that the department provides to them.[21] DOJ officials were not certain how all 9 staff would be divided across the training, oversight, technical security policy reviews, and other functions within SEPS. A SEPS official said that 3 of the 9 staff are to be allocated to oversight but noted that while the additional staff would help, they most likely would still not be enough to implement an effective classification management program. However, although DOJ includes SEPS in its departmentwide workforce analysis, that office has not separately determined the optimal level of resources needed to administer an effective security program. This is an important first step to resolving its resource constraints and complying with ISOO's recommendations.

In addition, SEPS does not have a strategy that lays out how it can best use anticipated resources to address the remaining deficiencies ISOO identified in ways that reduce the most risks to protecting national security information, such as whether to focus on addressing training, oversight, or other program gaps first. According to the program manager, with only 4 staff to cover departmentwide training and oversight issues, the office had not been able to be more proactive and strategic, achieving more comprehensive monitoring to prevent problems, and instead had to be more reactive and address classification concerns as they arose. In providing technical comments on a draft of the report, DOJ acknowledged that it has not conducted a formal assessment of the optimal level of resources SEPS needs to administer the information security program. DOJ also stated that SEPS identified in budget documents how the 9 additional staff would be allocated to address the remaining deficiencies identified by ISOO. However, DOJ provided no evidence of SEPS's strategy for allocating these additional staff.

Our previous work notes the importance of having a workforce analysis and developing a strategy to fill staffing gaps, both of which are characteristic of best practices followed by high-performing organizations. In *A Model of Strategic Human Capital Management*, we highlighted the importance of identifying current and future staffing needs, including the

[21] Established in 1975, the Working Capital Fund is a revolving fund authorized by law to finance a cycle of operations where the costs for goods or services provided are charged back to the recipient. The funds received are available for expenses and equipment necessary for maintenance and operation of such administrative services as the Attorney General, with the approval of OMB, determines may be performed more advantageously as central services. See 28 U.S.C. § 527. The fund is governed by an eight member Customer Advisory Board, which is chaired by the Assistant Attorney General for Administration, who is also the general manager of the fund.

appropriate number of employees and the correct mix of skills, for maximizing the value of employees and managing risk.[22] Also, we have emphasized that an essential element of effective workforce planning is aligning human capital strategies to eliminate gaps.[23] We have previously recommended that specific agencies adopt these practices. For instance, in a 2001 review of the Environmental Protection Agency (EPA), we recommended that EPA direct its major program offices to perform workforce analyses and then focus hiring and recruitment to fill any identified gaps.[24] Similarly, we recommended in 2003 that the Government Printing Office complete a workforce analysis to identify gaps in skills and competencies and develop strategies to address any gaps.[25] SEPS might benefit from adopting these human capital practices as part of a broad strategy to respond to ISOO's recommendations.

The FBI Has Begun to Implement All but One of ISOO's Recommendations

The FBI has begun or completed actions on all but one of ISOO's recommendations to correct several deficiencies ISOO identified in the FBI's classification management program.[26] These deficiencies included outdated policy guides for classifying information, insufficient training and program oversight, and improper marking of classified information. In its April 2005 final report, ISOO recommended that the FBI take 12 associated corrective actions. As of August 2006, the FBI had fully implemented 4 and had actions under way to implement 7 more, as shown in table 2.

[22] GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

[23] GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[24] GAO-01-812.

[25] GAO, *Government Printing Office: Advancing GPO's Transformation Effort through Strategic Human Capital Management*, GAO-04-85 (Washington, D.C.: Oct. 20, 2003).

[26] ISOO made 12 recommendations to FBI in its April 2005 report. FBI security officials indicated that the agency did not agree with one of the recommendations—develop a graduated sanctions system with significant sanctions for repeat offenders—because FBI's Office of Professional Responsibility had already issued offense and penalty tables that cover security violations. In addition, FBI's *Security Policy Manual* describes the consequences that individuals will be subjected to for disclosing classified information to unauthorized persons, such as sanctions identified in the *Offense Table and Penalty Guidelines Relating to the Disciplinary Process*, effective November 1, 2004.

Table 2: Status of the FBI's Implementation of ISOO's Recommendations as of August 2006

ISOO's recommendations to the FBI	
	Fully implemented
1.	Promulgate regulations to implement the classification management requirements of the executive order and ISOO's directive.
2.	Institute both annual self-inspections of the classification management program by the chief security officers and staff assistance visits by the Security Division.
3.	Publish and promulgate regulations for processing security violations, such as the unauthorized disclosure of classified information.
4.	Require that the Security and Inspection Divisions collaborate at least annually to evaluate the effectiveness of security inspections, which include reviews of classification program compliance, determine locations to be inspected, and make changes to their inspection checklist.
	Partially implemented
5.	Complete the update of the classification guides to encompass the FBI's expanded mission and to meet the requirements of the executive order.
6.	Develop a declassification guide, required by the executive order, to permit exemptions from automatic declassification requirements and submit it for approval.
7.	Ensure that all employees receive sufficient annual refresher training on classification management practices on a continuing basis.
8.	Update the FBI's outdated training for those staff with authority to originally classify information so as to reflect the current executive order.
9.	Provide refresher training in marking requirements to address discrepancies ISOO noted in its document review, and when the update of its primary classification guide is implemented, train all classifiers on its use and on the standards for classification.
10.	Review the number of staff with original classification authority in the Records Management Division, examine their role in classifying and declassifying information, and review the number of staff with this authority in the FBI as a whole to determine if the number can be reduced.
11.	Review and update the FBI's automated marking mechanisms (macros) in its electronic systems to ensure they are applying up-to-date markings.
	Disagreed with recommended change
12.	Develop a system that imposes graduated sanctions on those staff who repeatedly violate program requirements.

Source: GAO analysis of FBI information.

The FBI implemented 3 of ISOO's recommendations—those addressing security regulations, self-inspections, and the processing of security violations—by issuing its *Security Policy Manual* in December 2005, laying out responsibilities, policies, and procedures for implementing its classification management program. For a fourth completed recommendation—evaluating the effectiveness of security inspections—FBI's Security Division recently established the requirement that chief

security officers conduct annual self-inspections of their divisions' classification management programs and that Security Division staff conduct site visits to provide assistance where the head of the Security Division or another FBI division deems necessary.

As to the remaining 8 recommendations, the FBI disagreed with 1—to develop a graduated sanctions system for employees who repeatedly commit program violations—because it said that its Office of Professional Responsibility already had a system in place to apply such sanctions. Upon review of aspects of the sanctions system FBI has in place, ISOO officials agreed that it responds to this recommendation. The remaining 7 recommendations have been partially implemented, as discussed below.

Updated and Completed Classification Program Guidance

ISOO reported that the guides the FBI had in place to help employees make classification decisions neither contained current information nor reflected changes in the FBI's mission, particularly the increase in its intelligence capacity after the terrorist attacks of September 11, 2001. ISOO recommended the guides be updated. One had not been revised for 9 years, even though ISOO's directive implementing the executive order governing classified information calls for updates at least every 5 years. Classification guides are key to helping ensure employees have current, clear, and consistent guidance to make decisions about what information needs to be protected and restricted and what information can be released and shared, according to ISOO. FBI had complied with this recommendation for most of its guides. Security officials stated that although it had drafted an update of its primary classification guide, entitled *Foreign Counterintelligence Investigations Classification Guide*, it had not yet been issued because ongoing discussions between the FBI and DOJ's Office of Intelligence Policy and Review about various intelligence-related issues will affect the guide's content. As of August 2006, the FBI officials did not know when these issues would be resolved.

ISOO also found that the FBI lacked a guide for how to declassify documents, as the executive order requires and recommended that the FBI develop such a guide and submit it to the Interagency Security Classification Appeals Panel (ISCAP) for approval. According to FBI security officials, the guide has been drafted but not issued because the bureau was responding to panel comments on the draft. This guide is important because, among other things, it was to formally establish those exemptions the FBI could use when reviewing records to comply with the December 31, 2006, automatic declassification mandate. Delays in issuing the guide and establishing exemptions make it difficult for FBI to have

time to complete its review because of the volume of records it has to address, which could be as many as 110 million records, according to bureau estimates. ISOO noted that the FBI has taken positive steps to try to meet the date, such as drafting its declassification guide, identifying information that it could present to ISCAP for exemption from the automatic declassification requirement, and authorizing bulk declassification of documents.[27] But even with these initiatives, the bureau could still have up to 30 million records to review, which is why delays in issuing the guide and establishing exemptions may hinder completion of this review. As a result, some information that should remain protected could be available for public release, although the FBI could still try to reclassify it, deny release to protect individual privacy rights, or deny release for other reasons, such as to protect the identity of individuals who provide intelligence information to the government.

Updated Training on Classification and Marking Procedures

ISOO reported that although the FBI had some very sound training tools and to some extent provided excellent training, it was not thorough and offered consistently across the bureau. Specifically, ISOO reported that the amount and level of refresher training varied considerably among the FBI divisions, noting that the Counterintelligence and Counterterrorism Divisions' training was substantial and met the requirements of the executive order, in contrast to the Office of Intelligence, which did not provide adequate training as its refresher training included only a few minutes on security awareness. ISOO recommended that the FBI ensure that all employees with security clearances receive sufficient annual refresher training on the classification program. In response, FBI security officials stated that the agency has instituted a security awareness program that includes the refresher training, which is offered continuously rather than annually. The training is provided through means such as posting security tips as well as classification and marking materials on the FBI's intranet; having chief security officers distribute security awareness materials to employees; and providing live presentations and webcasts to all employees on classifying and marking practices. Although FBI has made this material available, it acknowledged that it does not have a system in place to track and ensure that all employees have received the

[27] All requests for exemptions from automatic declassification are to be submitted to the Interagency Security Classification Appeals Panel, which is composed of senior-level representatives from various agencies that handle the largest volume of classified information, at least 180 days before the automatic declassification date. All exemptions are to be approved, denied, or amended by this panel.

information because, according to FBI, tracking would be administratively burdensome considering the methods used to convey the information, which is not consistent with ISOO's directive. The directive requires agencies to maintain records of the training programs offered and employees' participation in them.

ISOO also noted that the FBI had outdated and insufficient training materials for those staff who are the primary classifiers of information, known as original classification authorities. ISOO found that the FBI's practice of waiting for these classifiers to contact the Security Division with questions about their responsibilities does not ensure they have a complete understanding of their role, as well as the executive order and implementing directives, and that this was critical since these individuals determine whether information meets the standards of potential damage to national security and should be classified. ISOO recommended that the FBI update this training, and the FBI expects to do so but is waiting until its classification and declassification guides are issued so that it can cover them in the training. FBI security program managers point out that more and more, these individuals are making declassification rather than classification decisions, and have been getting some training on their responsibilities for these decisions through one-on-one training, electronic communications, and participation in related training programs.

In almost half of the 575 classified FBI documents ISOO reviewed, it found marking errors. For example, ISOO found that portions of 110 documents (19 percent) appeared to be unnecessarily classified, while another 8 (1 percent) were clearly overclassified. To help eliminate these discrepancies, ISOO recommended that employees be provided refresher training on marking requirements and classifiers be trained in the updated classification guide when implemented. Otherwise, an ISOO official said, without proper guidance, employees tend to take a conservative approach and err on the side of classifying information. As we noted, the FBI has incorporated marking requirements in the refresher training and does plan to provide training on the new guides.

Review the Number of Staff with Classification Decision Authority

ISOO also recommended that the FBI review the number, roles, and responsibilities of those staff with original classification authority to determine if the number could be reduced. ISOO made this recommendation, in part, because it found that the percentage of staff with this authority within the FBI's Records Management Division, a support office, was higher than that for other executive branch agencies. According to FBI security officials, the number of staff with this authority

has been reduced in the Records Management Division and in the FBI as a whole. However, they said they will still have to re-examine the role of original classification authorities once the new guides are approved and issued.

Review and Update Automated Marking Mechanisms

ISOO also found missing, incomplete, or improper declassification markings in 176 of the documents (31 percent), but for most of these documents, about 80 percent, the errors were due to the fact that the FBI's automated marking mechanism (computer macro) was erroneously applying outdated codes that exempted information from being declassified. ISOO recommended that the FBI review and update its macro to ensure it is applying current codes, and FBI security officials reported they are testing updated macros and expect to implement them by the end of September 2006.

DOJ Components Lack Specific Guidance, Training, and Oversight to Ensure Proper Designation of Sensitive but Unclassified Information

The five components we reviewed had orders and directives in place to identify the various types of categories of sensitive but unclassified information they used and to describe how information should be handled and protected. However, none of these components had specific guidance in place to help ensure employees properly designate information as sensitive. DOJ indicated that it is waiting for the results of a governmentwide working group that will determine what designations agencies are to use before considering any modifications to how it manages this type of information. In addition to a lack of specific guidance, the components do not have other key internal controls in place to provide reasonable assurance that designations are being consistently applied—specifically, formal training on how to make decisions on when to apply the designations or perform oversight, such as assessments of how well their practices are working. Having these controls—specific guidance, training, and oversight—in place is important, considering that these components share information formally and informally with various federal and nonfederal entities, such as state and local law enforcement agencies. Without such controls, errors could occur and materials could be restricted unnecessarily or information that should be withheld could be disseminated.

DOJ Components Lack Specific Guidance for Sensitive but Unclassified Decision Making

All five DOJ components in our review developed general policy guidelines, such as orders and directives, in addition to a 1982 order, *Control and Protection of Limited Official Use Information*, which established a departmentwide policy for protecting sensitive but unclassified information. However, the five DOJ components we reviewed do not have specific guidance to help employees determine how to apply their sensitive but unclassified designations. Additionally, our governmentwide review of agencies' sensitive but unclassified designation practices also points to the importance of having formal, written guidance to give agency personnel a consistent understanding of whether and when to apply such designations, and we recommended in our March 2006 report that the Office of Management and Budget ensure agencies have this internal control in place. Written guidance is important because, according to the *Standards for Internal Control in the Federal Government*, information must be communicated in a suitable form and in a timely manner to those within an organization who need it to carry out their responsibilities. Furthermore, on the basis of our previous recommendations, other federal agencies have taken initiatives to enhance their guidance for their sensitive but unclassified designation processes. For example, earlier this year, the Department of Energy agreed with a recommendation we made to clarify its guidance on this subject and said that it is also planning ways to explicitly define for its employees what would be an inappropriate application of the sensitive but unclassified designations so that information is properly designated and handled.[28] Similarly, in part because of our past recommendation to the Department of Homeland Security's Transportation Security Administration, that office has begun to develop internal guidance that expands its existing regulations for sensitive security information—a category of sensitive but unclassified information—by providing personnel with examples of the types of information that should fall within various categories of sensitive security information.[29] By taking similar actions, DOJ could reduce the likelihood of errors and inconsistencies in applying the sensitive but unclassified designations throughout the department.

The existing policy guidelines for the five components we reviewed do not provide employees the level of specificity needed to adequately guide their decision making on applying the designation. For example, in its policy, the Drug Enforcement Administration's (DEA) definition of sensitive

[28] GAO-06-369.

[29] GAO-05-677.

information includes any information and materials that are investigative in nature, critical to the operation and mission of the agency, would violate a privileged relationship, or have its access restricted by law. However, the policy provides no explanation, guidance, or examples of the information that would meet any of these criteria, for instance, information that could be categorized as critical to DEA's mission. Similarly, the FBI's *Intelligence Policy Manual* sets forth definitions of various sensitive but unclassified categories, such as Law Enforcement Sensitive and For Official Use Only, but does not have specific guidance for designating documents, such as identifying the criteria for determining whether text in a document should be Law Enforcement Sensitive because, for example, it is associated with an ongoing criminal investigation. Finally, neither DEA nor FBI guidance contains examples of inappropriate applications of sensitive but unclassified designations. Without explicit language identifying appropriate and inappropriate use of the designation, DOJ components cannot be confident that their personnel are making correct and consistent decisions.

Moreover, the components in our review use five different sensitive but unclassified designations, as table 3 shows.

Table 3: Sensitive but Unclassified Categories Used by Five DOJ Components

FBI	DEA	USMS	ATF	Criminal Division
Limited Official Use (LOU)	Limited Official Use (LOU)	Limited Official Use (LOU)	Limited Official Use (LOU)	Limited Official Use (LOU)
For Official Use Only (FOUO)	Law Enforcement Sensitive (LES)	Law Enforcement Sensitive (LES)	For Official Use Only (FOUO)	Law Enforcement Sensitive (LES)
Law Enforcement Sensitive (LES)	DEA-Sensitive (DEA-S)		Law Enforcement Sensitive (LES)	
Proprietary Information (PROPIN)				

Source: GAO analysis of information provided by DOJ components.

Within a single DOJ component, employees could be confronted with making decisions on the sensitive but unclassified designation that might involve up to four categories, each with its own unique definition and safeguarding requirements, yet not have specific guidance on the types of information that merit each designation. For example, an employee at DEA can designate information Limited Official Use (LOU), Law Enforcement Sensitive, or DEA Sensitive (DEA-S), and each has different requirements. DEA requires administrative controls and additional safeguards for storage and transmission of DEA-S information that is equivalent to those for classified information. This means that DEA-S

information must be locked, for example, in a General Services Administration (GSA)-approved security container when not in the custody of an individual with a need to know that information. The LOU category, however, carries less stringent handling requirements that do not, for example, involve storing documents in a GSA-approved locked cabinet. Consequently, in such an instance, information that would warrant the DEA-S protection may not be adequately safeguarded from unintended disclosure. This underscores the need for employees to have specific guidance and examples to use to be able to clearly determine which information should be protected under these categories.

According to DOJ security officials, additional changes affecting the departmentwide guidance on sensitive but unclassified policies and procedures have been suspended pending the results of efforts connected to a December 2005 presidential memorandum.[30] This calls for, among other things, the development of standardized procedures across the federal government for designating, marking, and handling sensitive but unclassified information, in part, to promote effective and efficient use and sharing of this information. In general, the memorandum requires executive departments and agencies to inventory and assess their sensitive but unclassified procedures and determine the underlying authority for each procedure. For example, it mandated the submission of recommendations to the President for standardizing sensitive but unclassified procedures across the federal government for homeland security, law enforcement, and terrorism information, and the recommendations are expected by the end of December 2006. Once governmentwide standards have been established and a final decision is made on what sensitive but unclassified designations DOJ and its components will use, it will be important for them to develop specific guidance for employees that provides them with a clear understanding about when to apply each designation to ensure information is properly designated.

[30] Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment, December 16, 2005.

Training and Oversight for Their Designation Programs Are Limited for Selected DOJ Components

Federal internal control standards discuss the need for both training and continuous program oversight as necessary elements to ensure effective program implementation. However, training for the sensitive but unclassified designation process is lacking for the five DOJ components we reviewed. Although the Criminal Division and DEA offer training on handling and protecting sensitive but unclassified documents and material as part of periodic security awareness briefings, this training does not cover how to decide what information merits the designation. Specifically, security officials at the Criminal Division reported that the unit's classification briefing includes a section on sensitive but unclassified information. However, this training only provides employees with a definition of the various categories of information, such as grand jury information, informant and witness information, and investigative material, and not specific guidance on how to determine if specific information qualifies for one of these categories. Similarly, DEA provides employees computer-based training and briefings but only to convey information on handling, but not designating, sensitive but unclassified information. Without such training, employees may be at higher risk of improperly designating or not designating information as sensitive but unclassified. We have previously recommended that other agencies develop training to cover designation of sensitive but unclassified information, and all have agreed to initiate such training.[31]

In addition to having limited training programs, none of the components we reviewed have formally established policies and procedures regarding how they will monitor employees' appropriate and consistent application of sensitive but unclassified designations. Federal internal control standards call for, among other things, ensuring that ongoing oversight—such as self-inspections and supervisory reviews—occurs in the course of normal operations. The lack of such internal controls over sensitive but unclassified designations increases the potential that different components could designate the same information differently without detecting inconsistencies. Some components told us they rely on their unit's periodic security compliance reviews to assess how sensitive but unclassified information is handled and protected. However, some of these reviews have been conducted at up to 3-year intervals and, according to DEA security officials, are not designed to verify the accuracy of employees' sensitive but unclassified decisions. On the basis of our previous work, other agencies have acknowledged the role of effective

[31] See GAO-06-369 and GAO-05-677.

oversight procedures for the designation process and have taken actions to implement our recommendations to strengthen their procedures. For example, the Department of Defense and the Department of Energy, in response to our recommendations, have agreed to include oversight reviews of the sensitive but unclassified process as part of their routine security oversight assessments. Without similar actions, DOJ does not have reasonable assurance that the designations are applied accurately and consistently throughout the department.

The lack of guidance, training, and oversight is of particular concern in three of the five components we reviewed because these components do not limit the number of employees who can designate information as sensitive but unclassified. ATF and DEA restrict those authorized to make designations to a limited number of senior level employees. At the other components, however, any employee at any level is authorized to make these decisions. For example, at the FBI, any employee or contractor in the course of performing assigned duties may designate information Law Enforcement Sensitive. Yet in these components, employees do not have guides to consult and adequate training to help them make decisions on which information warrants a sensitive but unclassified designation, and the agencies do not have processes in place to oversee employee decision making in these instances. This increases the risk of inadvertent disclosure of information that should be protected or unintentional restriction of information needed to assist other governmental entities involved in criminal investigations or antiterrorism activities, or the unwarranted withholding of information from the public.

DOJ Components Report Having Processes in Place for Responding to Intragovernmental Information Requests

Information may be shared among federal entities through both formal and informal channels. One method for sharing information among Congress, executive agencies, and other federal entities is in response to formal requests from one federal entity to another. Each of the components in our review reported having processes in place for responding to intragovernmental requests for classified and sensitive but unclassified information, and the processes are consistent with federal internal control standards, although we did not independently test the effectiveness of these controls. For example, all of the components have central offices for receiving intragovernmental requests, involve subject matter experts in determining whether information can be disseminated, and conduct supervisory reviews of responses prior to release.

DOJ Components Report Having Central Offices for Receiving Intragovernmental Information Requests and Involving Subject Matter Experts in Determining How to Respond

Information may be shared among federal entities through both formal and informal channels. For instance, four of the DOJ components in our review reported that their employees share information informally with their counterparts at other federal agencies as part of everyday operations. Intragovernmental information requests are another, more formal method for sharing information. Four of the five components reported having central offices for receiving such requests from both Congress and executive agencies. DEA has a central office for receiving congressional, but not executive agency, requests. The use of central offices is consistent with federal standards for internal control, which note the importance of having clearly defined areas of responsibility in an organization. For example, USMS's Office of Congressional Affairs receives requests from Congress, while its Executive Secretariat receives executive agency requests. After a component's central office receives a request, it reviews the request to determine which subcomponent office has the knowledge necessary to respond and forwards it to that office.

From there, all of the components report using internal subject matter experts who have the relevant expertise to identify and assess material that would be used to respond to a request. This is also consistent with federal internal control standards that discuss the importance of ensuring that tasks are performed by the right employees. The subject matter experts rely on various resources as they decide how to respond. For example, these individuals might consult with other knowledgeable agency personnel. ATF employees may consult subject matter experts, such as the Office of Chief Counsel, and USMS staff may consult with the Office of General Counsel and division security officers.

Subject matter experts may consider several factors as they determine how to respond to a request, according to program officials at the components. At ATF, for instance, different factors are taken into account for different types of information, such as investigative records, tax information, or criminal informant records. DEA experts consider the content and sensitivity of the information, how the information will be used by the receiving entity, and the time frame for providing a response to determine how to respond to a request. In addition, at the Criminal Division, subject matter experts use their professional judgment to determine which factors to consider.

ATF, the Criminal Division, and the FBI reported having documented processes to guide their staff in responding to intragovernmental information requests, although these documents do not provide detailed guidance because components decide on how to respond on a case-by-

case basis. For instance, the Criminal Division cited the *Departmental Executive Secretariat Correspondence Policy, Procedures, and Style Manual* as providing written guidelines on responding to intragovernmental requests, although this manual does not include any guidance on what factors to consider during the decision-making process or how to determine whether information may be released to a requester. According to the components, the response process may differ for various reasons, such as the nature of the request and the requester's needs. For example, for a classified information request, a component may communicate with the requester to determine if an unclassified version of the information would satisfy the requester's information needs. Therefore, formal written policies may not always be helpful, given the need for a case-by-case approach to responses.

All of the Components Report Conducting Supervisory Reviews of Responses

After the subject matter experts have determined how to respond to the information request, all of the components report conducting a supervisory review before releasing the response; this corresponds to federal internal control standards that highlight the importance of management reviews for achieving effective results. At the FBI, a response may also undergo a review to determine if the information should continue to carry any classification or sensitive but unclassified designation after it is released. DEA and Criminal Division have processes for supervisory review that may vary depending on the nature of the request, according to officials at those components. At the Criminal Division, for instance, designated officials in the division determine who should review the information based on the nature of the request; reviews may be conducted by the Section Chief, Office Director, the Chief of Staff, and the Deputy Chief of Staff, among others. At DEA, the review process varies depending on which office owns the information that is responsive to the request and the nature of the request. According to DEA, executive agencies' requests that may be satisfied by information that is not sensitive may be approved by a unit chief, but the release of a response that contains sensitive information may require the approval of a section chief. Similarly, responses with highly sensitive information, such as information related to ongoing investigations or undercover operations, may require the approval of a senior executive at DEA.

All of the Components Report Communicating with Requesters during the Response Process, but the Level of Communication Varies by Request

All of the components reported that they communicated with requesters during the response process, which is consistent with federal internal control standards that note the importance of communicating with external stakeholders. Depending on the component, different offices communicate with requesters. At the FBI, the Office of Congressional Affairs may contact the congressional committee that requested information to obtain clarification about what is being requested. At the Criminal Division and DEA, however, experts within the relevant program office will contact the requester directly if clarification is needed. According to DEA officials, if the program office finds that the responsive information is classified or sensitive but unclassified, it may contact the requester to determine whether an unclassified or nonsensitive version of the information would be sufficient. For example, DEA might offer to provide an overview of an investigation, rather than a detailed description of the law enforcement techniques used during the investigation. All of the components reported that they inform requesters if information will be withheld or redacted prior to release. At the FBI, redacted information is usually assigned a deletion code, which explains the reason for the redaction, and according to agency officials, it provides congressional requesters with a deletion code sheet that describes the reasons for any redactions.

Conclusions

DOJ and FBI have made progress in implementing ISOO recommendations that help to strike a balance between the need to protect and the need to share critical information. FBI was taking action on almost all of ISOO's recommendations, and if it completes them, this will help to lower program risk, since FBI makes 98 percent of the classification decisions at DOJ. On the other hand, DOJ's program will remain at risk until DOJ addresses the most critical recommendation—providing sufficient resources. This is important because DOJ sets policy, provides training, and conducts oversight of classification management across the department and its components. SEPS's efforts to resolve staff limitations by acquiring additional resources through DOJ's Working Capital Fund may still not guarantee its needs are met because it is not certain it will get these resources, and even if it does, the security office does not know the optimum number of staff resources required to carry out its responsibilities. Furthermore, DOJ has not provided evidence of how SEPS will use the anticipated resources to perform various functions or of SEPS's strategy for how best to use these resources to address the remaining deficiencies ISOO identified in ways that reduce the most risks to protecting national security information, such as whether to focus on addressing training, oversight, or other program gaps first. Developing a

strategy, based on thoughtful workforce analysis and identification of gaps, would give SEPS a solid foundation on which to base its resource decisions to help perform its responsibilities, including implementing the remaining ISOO recommendations.

Moreover, without policies and procedures to provide specific guidance, training, and oversight for managing sensitive but unclassified information, DOJ cannot have reasonable assurance that this information is properly restricted or disclosed. Although DOJ is waiting for the results of the interagency working group before proceeding with additional changes to its program, it is important that DOJ ensures that its sensitive but unclassified designation practices provide its employees with the tools they need to apply designations appropriately. These tools include specific guidance, systematic training, and effective internal controls for overseeing compliance with policies and guidance. Identifying and designating documents properly is vital for not only preventing potential damage to governmental, commercial, or private interests, but also for sharing information, particularly with law enforcement entities that need it to protect the homeland.

Recommendations for Executive Action

To strengthen DOJ's management of classified information, we recommend that the Attorney General direct the SEPS director to take the following two actions:

- determine the resource level needed to ensure that it can effectively carry out the office's responsibilities, including full implementation of the ISOO recommendations; and

- devise a strategy for making resources available and for using them most effectively to address remaining deficiencies in ways that reduce the most risk to proper management of classified information, such as determining whether to address training, oversight, or other program deficiencies first.

In addition, to help ensure that sensitive but unclassified designations are correctly and consistently applied, we recommend that once the interagency working group has determined the standard set of sensitive but unclassified designations for the federal government, the Attorney General ensure that the department and its various components take the following three actions:

- establish specific guidance for applying the designations they will use,
- ensure that all employees authorized to make the designations have the necessary training before they can designate documents, and
- set internal controls for overseeing sensitive but unclassified designations to help ensure that they are properly applied.

Agency Comments and Our Evaluation

We provided a draft of this report to DOJ for review and comment. DOJ provided only written technical comments on the draft, which we incorporated, as appropriate. In providing these comments, DOJ stated that it generally agreed with the report and recommendations, and upon receipt of the final report, it will provide a response to our recommendations directly to Congress, as required by statute.

As agreed with your office, unless you publicly release its contents earlier, we plan no further distribution of this report until 30 days from its issue date. At that time, we will send copies of this report to the appropriate congressional committees and subcommittees, the Attorney General, and other interested parties. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-6510 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Sincerely yours,

Eileen Larence
Director, Homeland Security
and Justice Issues

Appendix I: Summaries of Related GAO Reports

This appendix summarizes the results of several related recently issued reports on agencies' programs for sharing classified and sensitive information and designating information as sensitive but unclassified. In June 2006, we issued two reports: one on the Department of Defense's classification management program and its effectiveness in minimizing classification errors[1] and the other on the status of the Department of Energy's classification management program.[2] We also issued two reports in March 2006: one on programs to safeguard sensitive but unclassified information at the Departments of Defense and Energy[3] and the other on the federal government's efforts to share terrorism-related and other sensitive but unclassified information among federal and nonfederal entities.[4] In June 2005, we issued a report on the designation of sensitive security information at the Transportation Security Administration.[5] These reports noted that policies and procedures governing classified and sensitive information require a number of enhancements to help ensure the effectiveness of information security programs. The highlights page for each of these reports is attached for more information.

[1] GAO-06-706.

[2] GAO, *Managing Sensitive Information: Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System*, GAO-06-785 (Washington, D.C.: June 30, 2006).

[3] GAO-06-369.

[4] GAO-06-385.

[5] GAO-05-677.

June 2006

MANAGING SENSITIVE INFORMATION

DOD Can More Effectively Reduce the Risk of Classification Errors

GAO 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

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.

United States Government Accountability Office

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-785, a report to the Chairman, Subcommittee on National Security, Emerging Threats and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

In recent years, the Congress has become increasingly concerned that federal agencies are misclassifying information. Classified information is material containing national defense or foreign policy information determined by the U.S. government to require protection for reasons of national security. GAO was asked to assess the extent to which (1) DOE's training, guidance, and oversight ensure that information is classified and declassified according to established criteria and (2) DOE has found documents to be misclassified.

What GAO Recommends

GAO is recommending that DOE conduct a similar number of classification oversight reviews, at a similar depth of analysis, as it did before the October 2005 shift in responsibility for classification oversight; apply selection procedures that more randomly identify classified documents for review; and disclose these selection procedures in future classification inspection reports.

DOE agreed with GAO's three recommendations but asserted it was already taking actions and making plans to ensure that the classification oversight program remains effective. Although GAO is encouraged by DOE's efforts, until the agency establishes a record of accomplishment under the new organizational structure, it will not be clear whether oversight will be as effective as it has been.

www.gao.gov/cgi-bin/getrpt?GAO-06-785.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gene Aloise, 202-512-3841, aloisee@gao.gov.

June 2006

MANAGING SENSITIVE INFORMATION

Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System

What GAO Found

DOE's Office of Classification's systematic training, comprehensive guidance, and rigorous oversight programs had a largely successful history of ensuring that information was classified and declassified according to established criteria. However, an October 2005 shift in responsibility for classification oversight to the Office of Security Evaluations has created uncertainty about whether a high level of performance in oversight will be sustained. Specifically, prior to this shift, the Office of Classification had performed 34 inspections of classification programs at DOE sites since 2000. These inspections reviewed whether DOE sites complied with agency classification policies and procedures. After the October 2005 shift, however, the pace of this oversight was interrupted as classification oversight activities ceased until February 2006. So far in 2006, one classification oversight report has been completed for two offices at DOE's Pantex Site in Texas, and work on a second report is under way at four offices at the Savannah River Site in South Carolina. More oversight inspections evaluating classification activity at eight DOE offices are planned for the remainder of 2006. In addition, according to the Director of the Office of Security Evaluations, the procedures for conducting future oversight are still evolving—including the numbers of sites to be inspected and the depth of analysis to be performed. If the oversight inspections planned for the remainder of 2006 are completed, it will demonstrate resumption in the pace of oversight conducted prior to October 2005. However, if these inspections are not completed, or are not as comprehensive as in the past, the extent and depth of oversight will be diminished and may result in DOE classification activities becoming less reliable and more prone to misclassification.

On the basis of reviews of classified documents performed during its 34 oversight inspections, the Office of Classification believes that very few of DOE's documents had been misclassified. The department's review of more than 12,000 documents between 2000 and 2005 uncovered 20 documents that had been misclassified—less than one-sixth of 1 percent. DOE officials believe that its misclassification rate is reasonable given the large volume of documents processed. Most misclassified documents remained classified, just not at the appropriate level or category. Of greater concern are the several documents that should have been classified but mistakenly were not. When mistakenly not classified, such documents may end up in libraries or on DOE Web sites where they could reveal classified information to the public. The only notable shortcomings we identified in these inspections were the inconsistent way the Office of Classification teams selected the classified documents for review and a failure to adequately disclose these procedures in their reports. Inspection teams had unfettered access when selecting documents to review at some sites, but at others they only reviewed documents from collections preselected by site officials. Office of Classification reports do not disclose how documents were selected for review.

United States Government Accountability Office

March 2006

MANAGING SENSITIVE INFORMATION

Departments of Energy and Defense Policies and Oversight Could Be Improved

GAO Highlights

Accountability · Integrity · Reliability

Highlights of GAO-06-369, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and Government Reform, House of Representatives

Why GAO Did This Study

In the interest of national security and personal privacy and for other reasons, federal agencies place dissemination restrictions on information that is unclassified yet still sensitive. The Department of Energy (DOE) and the Department of Defense (DOD) have both issued policy guidance on how and when to protect sensitive information. DOE marks documents with this information as Official Use Only (OUO) while DOD uses the designation For Official Use Only (FOUO). GAO was asked to (1) identify and assess the policies, procedures, and criteria DOE and DOD employ to manage OUO and FOUO information and (2) determine the extent to which DOE's and DOD's training and oversight programs assure that information is identified, marked, and protected according to established criteria.

What GAO Recommends

GAO made several recommendations for DOE and DOD to clarify their policies to assure the consistent application of OUO and FOUO designations and increase the level of management oversight in their use.

DOE and DOD agreed with most of GAO's recommendations, but partially disagreed with its recommendation to periodically review OUO or FOUO information. DOD also disagreed that personnel designating a document as FOUO should also mark it with the applicable FOIA exemption.

www.gao.gov/cgi-bin/getrpt?GAO-06-369.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Davi D'Agostino at (202) 512-5431 or Gene Aloise at (202) 512-3841.

What GAO Found

Both DOE and DOD base their programs on the premise that information designated as OUO or FOUO must (1) have the potential to cause foreseeable harm to governmental, commercial, or private interests if disseminated to the public or persons who do not need the information to perform their jobs and (2) fall under at least one of eight Freedom of Information Act (FOIA) exemptions. According to GAO's *Standards for Internal Control in the Federal Government*, policies, procedures, techniques, and mechanisms should be in place to manage agency activities. However, while DOE and DOD have policies in place, our analysis of these policies showed a lack of clarity in key areas that could allow for inconsistencies and errors. For example, it is unclear which DOD office is responsible for the FOUO program, and whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document. Also, both DOE's and DOD's policies are unclear regarding at what point a document should be marked as OUO or FOUO and what would be an inappropriate use of the OUO or FOUO designation. For example, OUO or FOUO designations should not be used to cover up agency mismanagement. In our view, this lack of clarity exists in both DOE and DOD because the agencies have put greater emphasis on managing classified information, which is more sensitive than OUO or FOUO.

While both DOE and DOD offer training on their OUO and FOUO policies, neither DOE nor DOD has an agencywide requirement that employees be trained before they designate documents as OUO or FOUO. Moreover, neither agency conducts oversight to assure that information is appropriately identified and marked as OUO or FOUO. According to *Standards for Internal Control in the Federal Government*, training and oversight are important elements in creating a good internal control program. DOE and DOD officials told us that limited resources, and in the case of DOE, the newness of the program, have contributed to the lack of training requirements and oversight. Nonetheless, the lack of training requirements and oversight of the OUO and FOUO programs leave DOE and DOD officials unable to assure that OUO and FOUO documents are marked and handled in a manner consistent with agency policies and may result in inconsistencies and errors in the application of the programs.

United States Government Accountability Office

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-06-385, a report to congressional requesters

March 2006

INFORMATION SHARING

The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information

Why GAO Did This Study

A number of initiatives to improve information sharing have been called for, including the Homeland Security Act of 2002 and in the Intelligence Reform and Terrorism Prevention Act of 2004. The 2002 act required the development of policies for sharing classified and sensitive but unclassified homeland security information. The 2004 act called for the development of an Information Sharing Environment for terrorism information.

This report examines (1) the status of efforts to establish government-wide information sharing policies and processes and (2) the universe of sensitive but unclassified designations used by the 26 agencies that GAO surveyed and their related policies and procedures.

What GAO Recommends

To provide for information-sharing policies and procedures, GAO recommends that the Director of National Intelligence (DNI) assess progress, address barriers, and propose changes, and that OMB work with agencies on policies, procedures, and controls to help achieve more accountability. OMB said that once ODNI completed its work, OMB would work with ODNI and all agencies on additional steps, if needed. ODNI declined to comment on our report, indicating that the subject matter is outside GAO's purview. We disagree with this assessment because it does not accurately reflect the scope of GAO's statutory authorities.

www.gao.gov/cgi-bin/getrpt?GAO-06-385.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner, 202-512-9286, pownerd@gao.gov or Eileen Larence, 202-512-6510, larencee@gao.gov.

What GAO Found

More than 4 years after September 11, the nation still lacks governmentwide policies and processes to help agencies integrate the myriad of ongoing efforts, including the agency initiatives we identified, to improve the sharing of terrorism-related information that is critical to protecting our homeland. Responsibility for creating these policies and processes shifted initially from the White House to the Office of Management and Budget (OMB), and then to the Department of Homeland Security, but none has yet completed the task. Subsequently, the Intelligence Reform Act called for creation of an Information Sharing Environment, including governing policies and processes for sharing, and a program manager to oversee its development. In December 2005, the President clarified the roles and responsibilities of the program manager, now under the Director of National Intelligence, as well as the new Information Sharing Council and the other agencies in support of creating an Information Sharing Environment by December 2006. At the time of our review, the program manager was in the early stages of addressing this mandate. He issued an interim implementation report with specified tasks and milestones to Congress in January 2006, but soon after announced his resignation. This latest attempt to establish an overall information-sharing road map under the Director of National Intelligence, if it is to succeed once a new manager is appointed, will require the Director's continued vigilance in monitoring progress toward meeting key milestones, identifying any barriers to achieving them, and recommending any necessary changes to the oversight committees.

The agencies that GAO reviewed are using 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect information that they deem critical to their missions—for example, sensitive law or drug enforcement information or controlled nuclear information. For most designations there are no governmentwide policies or procedures that describe the basis on which an agency should assign a given designation and ensure that it will be used consistently from one agency to another. Without such policies, each agency determines what designations and associated policies to apply to the sensitive information it develops or shares. More than half the agencies reported challenges in sharing such information. Finally, most of the agencies GAO reviewed have no policies for determining who and how many employees should have authority to make sensitive but unclassified designations, providing them training on how to make these designations, or performing periodic reviews to determine how well their practices are working. The lack of such recommended internal controls increases the risk that the designations will be misapplied. This could result in either unnecessarily restricting materials that could be shared or inadvertently releasing materials that should be restricted.

United States Government Accountability Office

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-GAO-05-677, a report to congressional requesters

Why GAO Did This Study

Concerns have arisen about whether the Transportation Security Administration (TSA) is applying the Sensitive Security Information (SSI) designation consistently and appropriately. SSI is one category of "sensitive but unclassified" information—information generally restricted from public disclosure but that is not classified. GAO determined (1) TSA's SSI designation and removal procedures, (2) TSA's internal control procedures in place to ensure that it consistently complies with laws and regulations governing the SSI process and oversight thereof, and (3) TSA's training to its staff that designate SSI.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct TSA to establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI; establish clear responsibility for the identification and designation of SSI information; establish internal controls monitoring compliance with its SSI regulations, policies, and procedures, and communicate that responsibility for implementing the controls throughout TSA; and provide specialized training to those making SSI designations on how information is to be identified and evaluated for SSI status. The Department of Homeland Security generally concurred with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-677.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Laurie E. Ekstrand at (202) 512-8777 or ekstrandl@gao.gov.

June 2005

TRANSPORTATION SECURITY ADMINISTRATION

Clear Policies and Oversight Needed for Designation of Sensitive Security Information

What GAO Found

TSA does not have guidance and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI or who can make the designation. Such guidance is required under GAO's standards for internal controls. In addition, TSA has no policies on accounting for or tracking documents designated as SSI. As a result, TSA was unable to determine either the number of TSA employees actually designating information as SSI or the number of documents designated SSI. Further, apart from Freedom of Information Act (FOIA) requests or other requests for disclosure outside of TSA, there are no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed.

TSA also lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA. Specifically, TSA has not established and documented policies and internal control procedures for monitoring compliance with the regulations, policies, and procedures governing its SSI designation process, including ongoing monitoring of the process. TSA officials told us that its new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. This office, which was established in February 2005, will also develop and implement all TSA policy concerning SSI handling, training, and protection. More detailed information on how this office's activities will be operationalized was not yet available. Specifically, TSA officials provided no written policies formalizing the office's role, responsibilities, and authority.

TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is identified and evaluated for protected status. Development of such training for SSI designations is needed to help ensure consistent implementation of the designation authority across TSA. While TSA has provided a training briefing on SSI regulations to certain staff, such as the FOIA staff, it does not have specialized training in place to instruct employees on how to consistently designate information as SSI. In addition, TSA has no written policies identifying who is responsible for ensuring that employees comply with SSI training requirements.

United States Government Accountability Office

Appendix II: Objectives, Scope, and Methodology

This report responds to the following questions:

1. To what extent has the Department of Justice (DOJ) implemented the Information Security Oversight Office's (ISOO) recommendations?

2. To what extent has the Federal Bureau of Investigation (FBI) implemented ISOO's recommendations?

3. What policies, procedures, and internal controls are in place in selected DOJ components to properly use sensitive but unclassified designations?

4. What processes are in place at selected DOJ components respond to intragovernmental requests to share national security and sensitive but unclassified information?

To determine the extent of changes DOJ and the FBI have made to implement ISOO's recommendations, published in July 2004 and April 2005, we reviewed the results of ISOO's audits; obtained supporting documents, when available, such as DOJ and FBI policy directives, orders, and guidance; and interviewed DOJ and FBI managers responsible for implementing and overseeing these programs. Although the results of ISOO's reviews are not necessarily generalizable to all classified documents at DOJ and the FBI, we assessed the methodology ISOO used to conduct its reviews and determined that it is adequate to support its recommendations. We also compared ISOO's recommendations and DOJ's and FBI's classified information practices to Executive Order 12958, as amended;[1] ISOO's Directive No. 1, entitled *Classified National Security Information*;[2] and our *Standards for Internal Control in the Federal Government*, as appropriate. We did not assess the effectiveness of the security education and training programs at DOJ and the FBI.

To determine the extent of policies, procedures, and internal controls that selected DOJ components have in place for designating information as sensitive but unclassified, we used our *Standards for Internal Control in the Federal Government* to provide criteria against which we assessed components' sensitive but unclassified designation policies and procedures. Moreover, we reviewed DOJ-specific data collected as part of

[1] See Exec. Order No. 13292, 68 Fed. Reg. 15,315 (Mar. 28, 2003).

[2] See 32 C.F.R. pt. 2001.

GAO's governmentwide review of 26 agencies' programs on sensitive but unclassified information.[3] These data consisted of written responses to a set of questions about the agencies' policies, procedures, and internal controls and any written documentation provided in support of these responses, such as policy and training manuals. We selected the five DOJ components included in this review—Bureau of Alcohol, Tobacco, Firearms and Explosives; Criminal Division; Drug Enforcement Administration; the FBI; and U.S. Marshals Service—because data collected as part of a GAO governmentwide review of sensitive but unclassified information indicated that each of these DOJ components had adopted one or more of this type of designation in addition to the departmentwide Limited Official Use designation. We conducted follow-up interviews with security officials and senior program officials in these five components to supplement information gathered as part of GAO's governmentwide review. We also examined individual components' written policies and procedures on sensitive but unclassified information, when available.

To determine how selected DOJ components respond to federal intragovernmental requests for classified and sensitive but unclassified information, we obtained documentation of their response processes from the five components, when available, and interviewed security officials and senior program officials. We compared their processes for responding to these requests to identify similarities and differences within and across the components and reviewed supporting documents, when available. We did not independently test the effectiveness of the processes components described to us.

We conducted our work from June 2005 through August 2006 in accordance with generally accepted government auditing standards.

[3] Twenty-six agencies were included in that review—24 of which are subject to the Chief Financial Officers Act and two others, the Federal Energy Regulatory Commission and the U.S. Postal Service because our previous experience with these agencies indicated that they used sensitive but unclassified designations.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Eileen Larence (202) 512-6510 or larencee@gao.gov

Staff Acknowledgments

In addition to the contact named above, Glenn Davis, Assistant Director; Cynthia Auburn; Kathryn Godfrey; David Hudson; Thomas Lombardi; Mary Martin; Terry Richardson; and Susan Tieh made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548