United States Government Accountability Office

GAO

Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

June 2006

MANAGING SENSITIVE INFORMATION

DOD Can More Effectively Reduce the Risk of Classification Errors

GAO-06-706

June 2006

MANAGING SENSITIVE INFORMATION

DOD Can More Effectively Reduce the Risk of Classification Errors

GAO Accountability · Integrity · Reliability

Highlights

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

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.

Contents

Tables

Figures

Abbreviations

DOD	Department of Defense
GAO	Government Accountability Office
ISOO	Information Security Oversight Office
OSD	Office of the Secretary of Defense
OUSD(I)	Office of the Under Secretary of Defense for Intelligence

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 30, 2006

The Honorable Christopher Shays
Chairman, Subcommittee on National Security, Emerging Threats,
and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The U. S. Government classifies information as Confidential, Secret, or Top Secret if its unauthorized disclosure could damage the national security of the United States.[1] Since 1940, the classification, safeguarding, and declassification of national security information have been prescribed in a series of presidential executive orders. The current order in effect, Executive Order 12958, *Classified National Security Information*, as amended, defines the different security classification levels, lists the types of information that can be protected, and describes how to identify and mark classified information.[2]

According to data compiled by the Information Security Oversight Office (ISOO), the office responsible for overseeing the government's information security program, the number of classified records in existence is unknown because there is no requirement to account for the majority of these records. However; during the last 5 fiscal years that data are available (2000 through 2004), federal agencies reported that they created about 110 million new classified records, of which the Department of Defense (DOD) was responsible for more than half (66.8 million).[3] The former DOD Deputy Under Secretary of Defense for Counterintelligence and Security testified in 2004 in a congressional hearing that she believed

[1]National security signifies the national defense or foreign relations of the United States.

[2]Executive Order 12958, *Classified National Security Information* (1995) with its last amendment, Executive Order 13292, *Further Amendment to Executive Order 12958*, as Amended, *Classified National Security Information* (2003).

[3]See title 44 United States Code, which generally defines a record as a book, paper, map, photograph, sound or video recording, machine readable material, computerized, digitized, or electronic information, regardless of the medium on which it is stored, or other documentary material, regardless of its physical form or characteristics.

the department overclassified information, and she estimated that 50 percent of information may be overclassified, to include overclassification between the classification levels. An example would be the classifying of information as Top Secret instead of Secret. The Director of ISOO in the same hearing testified that information that should not be classified is increasing, in violation of the Executive Order. According to the Director, too much classification impedes effective information sharing, too little classification can provide adversaries with information to harm the United States and its allies; and misclassification in general causes the department to incur millions of dollars in avoidable administrative costs.

The Under Secretary of Defense for Intelligence is the senior DOD official responsible for the direction, administration, and oversight of DOD's information security program.[4] DOD's current implementing regulation, *Information Security Program*, was issued in January 1997 and augmented with interim guidance in April 2004 to reflect changes required by Executive Order 12958, as amended. The regulation has decentralized the management of the program to the heads of the various DOD components.[5] Officials from the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) told us that they expect to publish an updated version of the *Information Security Program* in 2007 to replace the 1997 edition and the interim guidance.

As requested, we examined (1) whether the implementation of DOD's 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. As part of your request that we report on DOD's information security program, we also reported in March 2006 on the Department of Defense and Department of Energy programs to safeguard unclassified yet sensitive information and we will report on the status of the Department of Energy's information security

[4]The Under Secretary of Defense for Intelligence position was established by the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (Pub. L. No. 107-314 §901 (Dec. 2, 2002)).

[5]DOD components include the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General, the Defense Agencies, the DOD Field Activities, and all other organizational entities within DOD.

program later this year.[6] In similar work, we recently issued a report on the designation of sensitive security information at the Transportation Security Administration[7] and a report on the executive branch agencies' current efforts to share sensitive homeland security information among federal and nonfederal entities, and the challenges posed by such information sharing.[8] Finally, we are currently reviewing the management of both unclassified yet sensitive information and national security information within the Department of Justice.

To evaluate whether DOD's information security program effectively minimizes the risk of misclassification, the reliability of DOD's annual classification decision estimate, and the likelihood of DOD's meeting automatic declassification deadlines, we reviewed documentation and met with officials responsible for setting information security policy and implementation (such as training and oversight) from the OUSD(I) and nine DOD components and 10 of their subordinate commands. Collectively, these nine components are responsible for about 83 percent of the department's classification decisions. We compared the DOD components' and subordinate commands' information security policies and practices with the Executive Order 12958, as amended; the ISOO directive, *Classified National Security Information Directive No. 1*; the DOD regulation 5200.1-R, *Information Security Program*; and other DOD implementing guidance.

To assess adherence to procedures in the Executive Order for classifying information, we reviewed a nonprobability sample of 111 recently classified documents prepared by five offices within the Office of the Secretary of Defense (OSD). Because the total number of classified documents held by DOD is unknown, we did not pursue a probability

[6] *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved*, GAO-06-369 (Washington, D.C.: Mar. 7, 2006); *Managing Sensitive Information: DOE and DOD Could Improve Their Policies and Oversight*, GAO-06-531T (Washington, D.C.: Mar. 14, 2006).

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

[8] *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).

sampling methodology to produce results that could be generalized to OSD or DOD. [9]

We conducted our work between March 2005 and February 2006 in accordance with generally accepted government auditing standards. A more thorough description of our scope and methodology is provided in appendix I.

Results in Brief

A lack of oversight and inconsistent implementation of DOD's information security program increase the risk of misclassification. DOD's information security program is decentralized to the DOD component level, and the OUSD(I) has limited involvement in, and oversight of, components' information security programs. This office does little monitoring or evaluating of the DOD components' information security actions. Also, while some DOD components and subordinate commands appear to manage their programs effectively, we identified weaknesses in other components' and subordinate commands' training, self-inspection, and security classification guide management. For example, all of the DOD components and subordinate commands that we reviewed offered the compulsory initial and annual refresher training for personnel eligible to classify documents. However, classification management training at 8 of the 19 components and subordinate commands we reviewed did not cover fundamental classification management principles, such as the markings that must appear on classified information and the process for determining the duration of classification. Also, the OUSD(I) did not have a process to confirm whether required self-inspections had been performed or to evaluate their quality, and did not prescribe in detail what self-inspections should cover. We found that only 8 of the 19 DOD components and subordinate commands performed these required self-inspections. Instead, more than half of the 19 performed less rigorous staff assistance visits. We also found that some of the DOD components and subordinate commands that we examined did not routinely submit copies of their security classification guides, documentation which identifies what information needs protection and the reason for classification, to a central library as required. Some did not track their security classification guides to ensure they were current and reviewed every 5 years as required. As a result,

[9]Results from nonprobability samples cannot be used to make inferences about a population, because the chance of being selected as part of a nonprobability sample cannot be predicted.

DOD personnel cannot be assured that they are using the most current information to derivatively classify documents. DOD is studying ways to improve its current approach to making security classification guides readily available, departmentwide. Because of the lack of oversight and weaknesses in training, self-inspections, and 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.

Our review of a nonprobability sample of 111 classified DOD documents from five OSD offices shows that, within these offices, DOD personnel are not uniformly following established procedures for classifying information, to include correctly marking classified information. Executive Order 12958, as amended, lists criteria for what information can be classified, and which markings are required on classified records. In our review of the OSD documents, we questioned DOD officials' classification decisions for 29 documents—that is, 26 percent of the sample. The majority of our questions centered around two problems: the inconsistent treatment of similar information within the same document, and whether all of the information marked as classified met established criteria for classification. We also found that 93 of the 111 documents we examined (84 percent) had at least one marking error, and about half had multiple marking errors. For example, we found that 25 percent of the 111 documents had improper declassification instructions, and 42 percent of the documents failed to provide information about their data sources—such as the names and dates—as required. While the results from this review cannot be generalized across DOD, they are indications of the lack of oversight and inconsistency that we found in DOD's implementation of its information security program.

The accuracy of DOD's annual estimate of its number of classification decisions is questionable. Although ISOO issues guidance on how components should calculate their classification decisions estimate, we found considerable variance across the department and from year to year in how this guidance was implemented. For example, DOD components differed in the types of information they included in the count, the number and types of lower echelon units included in the count, and decisions as to when to count and for how long. In fiscal year 2005, OUSD(I) began scrutinizing the estimates of its components before consolidating and submitting them to ISOO for inclusion in its annual report to the President.

DOD's ability to meet all of the automatic declassification deadlines in Executive Order 12958, as amended, depends on the actions of other

federal agencies. DOD components reported being on pace to review their documents of permanent historical value by December 31, 2006; however, they told us that they are unlikely to review all of the documents referred to them by other DOD components and non-DOD agencies before 2010, and special media (such as audio and video recordings) before 2012, the dates on which these records are scheduled to be automatically declassified. DOD's progress in reviewing records that contain classified information belonging to other federal agencies is hampered by the absence of a federal government standard for annotating these records, a centralized location within DOD or the federal government to store these records, and, a common database that federal agencies can use to track the status of these records. DOD's ability to remove these impediments without the involvement of other federal agencies is limited. If DOD fails to complete its review by the declassification deadlines, it risks inappropriately declassifying information that should remain classified.

To reduce the risk of misclassification and improve DOD's information security operations, we are recommending six actions, including several to increase program oversight and accountability. In commenting on our draft, DOD agreed with all of our recommendations. DOD also provided technical comments, which we have included as appropriate. The department's response is reprinted in appendix II.

Background

Executive Order 12958, *Classified National Security Information*, as amended, specifies three incremental levels of classification—Confidential, Secret, and Top Secret—to safeguard information pertaining to the following:

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities (including special activities), intelligence sources/methods, cryptology;
- foreign relations/activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism;
- United States government programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
- weapons of mass destruction.

The requisite level of protection is determined by assessing the damage to national security that could be expected if the information were compromised (see table 1).

Table 1: Classification Level and the Expected Impact of Unauthorized Disclosure

Classification levels	Expected impact of unauthorized disclosure
Confidential	Damage
Secret	Serious damage
Top Secret	Exceptionally grave damage

Source: Executive Order 12958, §1.2, as amended.

Executive Order 12958, as amended, prohibits classifying information so as to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or agency; restrain competition; or prevent or delay the release of information, which does not require protection in the interest of national security.

Classification decisions can be either original or derivative. Original classification is the initial determination that information requires protection against unauthorized disclosure in the interest of national security. An original classification decision typically results in the creation of a security classification guide, which is used by derivative classifiers and identifies what information should be protected, at what level, and for how long. Derivative classification is the incorporation, paraphrasing, or generation of information in new form that is already classified, and marking it accordingly.[10] In 2004, 1,059 senior-level officials in DOD were designated original classification authorities, and as such, they were the only individuals permitted to classify information in the first instance.[11] But any of the more than 1.8 million DOD personnel who possess security clearances potentially have the authority to classify derivatively. According to DOD, less than 1 percent of the estimated 63.8 million classification decisions the department made during fiscal years 2000

[10]The duplication or reproduction of existing classified information is not derivative classification.

[11]Information may be originally classified only by the Secretary of Defense, the secretaries of the military departments, and other officials who have been specifically designated this authority in writing. By DOD regulation, delegation of original classification authority shall be limited to the minimum required for DOD to operate effectively, and to those officials who have a demonstrable and continuing need to exercise it.

through 2004 were original; however, ultimately, original classification decisions are the basis for 100 percent of derivative classification decisions.

Executive Order 12958, as amended, assigns ISOO the responsibility for overseeing agencies' compliance with the provisions of the Executive Order.[12] In this capacity, ISOO (1) performs on-site inspections of agency information security operations, (2) conducts document reviews, (3) monitors security education and training programs, and (4) reports at least annually to the President on the degree to which federal agencies are complying with the Executive Order. ISOO also issued *Classified National Security Information Directive No. 1* to implement the Executive Order.[13] The Executive Order and the ISOO directive stipulate a number of specific responsibilities expected of federal agencies, including DOD. Examples of responsibilities are promulgating internal regulations; establishing and maintaining security education and self-inspection programs; conducting periodic declassification reviews; and committing sufficient resources to facilitate effective information security operations. The Executive Order and the ISOO directive also require classifiers to apply standard markings to classified information. For example, originally classified records must include the overall classification as well as portion or paragraph marking, a "Classified by" line to identify the original classifier, a reason for classification, and a "Declassify on" date line.

Executive Order 12958, as amended, states that information shall be declassified when it no longer meets the standards for classification.[14] The point at which information generally becomes declassified is set when the decision is made to classify, and it is either linked to the occurrence of an event, such as the completion of a mission, or to the passage of time. Classified records that are more than 25 years old and have permanent historical value are automatically declassified unless an exemption is

[12]ISOO is a component of the National Archives and Records Administration and receives its policy and program guidance from the National Security Council.

[13]32 C.F.R. Part 2001 (2003).

[14]Executive Order 12958, as amended, defines declassification as the authorized change in the status of information from classified to unclassified.

granted because their contents could cause adverse national security repercussions.[15]

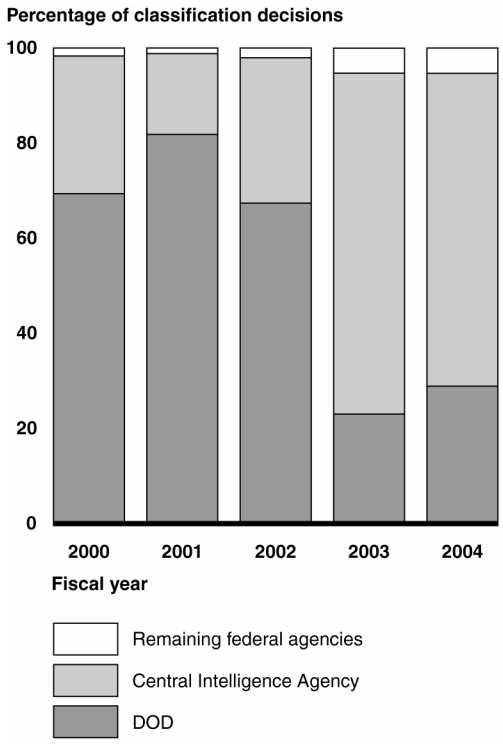
The Defense Security Service Academy is responsible for providing security training, education, and awareness to DOD components, DOD contractors, and employees of other federal agencies and selected foreign governments. The academy's 2005 course catalog includes more than 40 courses in general security and in specific disciplines of information, information systems, personnel, and industrial security, and special access program security. These courses are free for DOD employees and are delivered by subject matter experts at the academy's facilities in Linthicum, Maryland, and at student sites worldwide via mobile training teams. Some courses are available through video teleconferencing and the Internet. In fiscal year 2004, more than 16,000 students completed academy courses, continuing an upward trend over the past 4 years.[16]

According to ISOO, DOD is one of the most prolific classifiers (original and derivative combined) among federal government agencies. From fiscal year 2000 to fiscal year 2004, DOD and the Central Intelligence Agency had individual classification activity that were each more than all other federal agencies combined. In 3 of these 5 years, DOD's classification activity was higher than that of the Central Intelligence Agency's (see figure 1).

[15]Records of permanent historical value are Presidential records and agency records that the U.S. Archivist determines should be maintained permanently in accordance with title 44 United States Code.

[16]The actual number of students completing academy courses in fiscal year 2004 is less than 16,000 because some students completed multiple courses.

Figure 1: DOD's Number of Classification Decisions Compared to Those of Other Federal Agencies



Source: GAO's analysis of ISOO data.

During these same 5 years, DOD declassified more information than any other federal agency, and it was responsible for more than three-quarters of all declassification activity in the federal government.

DOD's Information Security Program Lacks Oversight and Consistent Implementation

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 OUSD(I) involvement in, and oversight of, components' information security programs is limited. Also, while some DOD components and subordinate commands appear to manage their programs effectively, we identified weaknesses in others' training, self-inspections, and security classification guide management. As a result, we found that many of the organizations we reviewed do not fully satisfy federal and DOD classification management requirements, which contributes to an increased risk of misclassification. Specifically, most of the components and subordinate commands we examined did not establish procedures to

ensure that personnel authorized to and actually performing classification actions are adequately trained to do so, did not conduct rigorous self-inspections, and did not take required actions to ensure that derivative classification decisions are based on current, readily available documentation. According to the ISOO Director, adequate training, self-inspections, and documentation are essential elements of a robust information security program and their absence can impede effective information sharing and possibly endanger national security.[17]

OUSD(I) Oversight of DOD Classification Management Program Is Limited

As required by Executive Order 12958, OUSD(I) issued a regulation in January 1997, *Information Security Program*, outlining DOD's information security program. This regulation does not specifically identify oversight responsibilities for OUSD(I), but instead decentralizes the management of the information security program to the heads of DOD components. Consequently, according to the DOD regulation, each DOD component is responsible for establishing and maintaining security training, conducting self-inspections, and issuing documentation to implement OUSD(I) guidance and security classification guides. OUSD(I) exercises little oversight over how the components manage their programs. As a result, OUSD(I) does not directly monitor components' compliance with federal and DOD training, self-inspection, and documentation requirements stipulated in Executive Order 12958, as amended; the ISOO directive; and the DOD regulation. For example, OUSD(I) does not require components to report on any aspects of the security management program. Also, OUSD(I) does not conduct or oversee self-inspections, nor does it confirm whether self-inspections have been performed or review self-inspection findings. At the time of our review, OUSD(I)'s involvement consisted of accompanying ISOO on periodic inspections of select DOD components and subordinate commands that are not under the four military services. Additionally the DOD implementing regulation does not describe what self-inspections should cover, such as the recommended standards in the ISOO directive.

Based on our analysis, we believe that OUSD(I)'s decentralized approach, coupled with the lack of specificity in the department's implementing regulation on what components must do to satisfy the Executive Order

[17]J. William Leonard, Director, ISOO. "The Importance of Basics," remarks delivered at the National Classification Management Society's Annual Training Seminar, Reno, Nevada, June 15, 2004.

and ISOO directive self-inspection requirement, has resulted in wide variance in the quality of components' information security programs.

Classification Management Training Is Inadequate to Substantially Reduce Improper Classification Practices

Because all cleared personnel have the authority to derivatively classify information, they are required to have annual refresher training, whether or not they engaged in derivative classification actions. All of the 19 DOD components and subordinate commands we reviewed offer initial and annual refresher training for their personnel who are involved with derivative classification activities, and most track attendance to ensure that the training is received, as required by the ISOO directive and the DOD regulation (see table 2).

However, from our analysis of the components' and subordinate commands' initial and annual refresher training, we determined that only 11 of the 19 components and subordinate commands cover the fundamental classification principles cited in the ISOO directive, the DOD regulation, and specifically defined as the minimum training that classifiers must have in a November 2004 memorandum signed by the Under Secretary of Defense for Intelligence.[18] That is, the training offered by 8 of the components and subordinate commands does not describe the basic markings that must appear on classified information, the difference between original and derivative classification, the criteria that must be met to classify information, and the process for determining the duration of classification. Consequently, this training will not provide DOD with assurance that it will reduce improper classification practices, as called for in the ISOO directive. We also noted that 14 of the DOD components and subordinate commands do not assess whether participants understand the course material by administering a proficiency test.

[18]Memorandum from Stephen A. Cambone, Under Secretary of Defense for Intelligence, "Minimum Training Requirements for Original Classification Authorities and Derivative Classifiers," Nov. 30, 2004.

Table 2: DOD Component Training Programs for Derivative Classifiers

DOD components and subordinate commands	Initial and annual refresher training	Participant attendance tracked	Classification principles adequately covered	Proficiency tested
Department of the Army	•	•	•	
Army Intelligence and Security Command	•	•	•	
Army Materiel Command	•	•	•	
Army Research Development and Engineering Command	•	•		
Chief of Naval Operations	•			
Naval Sea Systems Command	•			
Naval Surface Warfare Center, Dahlgren Division	•	•	•	•
Naval Air Systems Command	•	•		
Department of the Air Force	•	•		
Air Combat Command	•	•	•	
Air Force Materiel Command	•	•		
88th Air Base Wing	•	•	•	•
Headquarters, Marine Corps	•			
Marine Forces Atlantic	•	•		
Central Command	•		•	
Special Operations Command	•	•	•	•
National Geospatial-Intelligence Agency	•	•	•	•
Defense Intelligence Agency	•	•	•	•
National Security Agency	•		•	

Source: GAO's analysis of DOD data.

Components and subordinate commands that cover the classification principles cited in the ISOO directive and the DOD regulation include:

- the Army Intelligence and Security Command, which issues the Command's *A Users Guide to the Classification and Marking of Documents* to personnel;

- the Army Materiel Command, which uses information obtained from the Defense Security Service Academy to develop its refresher training on marking classified records;
- the Naval Surface Warfare Center, Dahlgren Division, which requires personnel to complete an online refresher course and pass a proficiency test before they can print out a certificate indicating a passing score;
- the 88th Air Base Wing, which requires personnel to attend four quarterly briefings each year on relevant classification management topics;
- the Special Operations Command, which developed an online refresher course, complete with a proficiency test that must be passed to receive credit for attending;
- the National Geospatial-Intelligence Agency, which requires personnel to sign an attendance card indicating that they completed initial and annual refresher training, and issues them the agency's *Guide to Marking Documents*; and
- the Defense Intelligence Agency, which provides personnel a 13-page reference guide that explains how to comply with Executive Order 12958, as amended.

All of the components and subordinate commands that we examined provide their original classification authorities with initial training, frequently in one-on-one sessions with a security manager. However, only about half of the components and subordinate commands we examined provide the required annual refresher training to original classification authorities.

DOD personnel could take better advantage of the information security curriculum offered by the Defense Security Service Academy, including *Basic Information Security*, *Information Security Orientation*, *Information Security Management*, and *Marking Classified Information*. For example, *Marking Classified Information* is a 2-3 hour no-cost, online course that explains how to mark classified information in accordance with Executive Order 12958, as amended, and requires the person taking the course to complete and pass a proficiency test at the end of the course. The Under Secretary's memorandum specifically mentioned the academy and its courses as a way for the components to facilitate their training. Our analysis of academy attendance data for fiscal years 2003 through 2004 indicates that of the more than 1.8 million DOD personnel who possessed security clearances and potentially had the authority to classify documents derivatively, 4,775 DOD personnel completed an information security

course, and 2,090 DOD personnel completed the *Marking Classified Information* course.[19, 20]

Self-Inspections Lack Rigor

Eleven of the 19 DOD components and subordinate commands we reviewed do not perform required self-inspections as part of the oversight of their information security programs. The ISOO directive requires agencies to perform self-inspections at all organizational levels that originate or handle classified information. Agencies have flexibility in determining what to cover in their self-inspections, although ISOO lays out several standards that it recommends DOD and other agencies consider including, such as:

- reviewing a sample of records for appropriate classification and proper markings;
- assessing familiarity with the use of security classification guides;
- reviewing the declassification program;
- evaluating the effectiveness of security training; and
- assessing senior management's commitment to the success of the program.

In its *Information Security Program* regulation, DOD components are directed to conduct self-inspections based on program needs and the degree of involvement with classified information; components and subordinate commands that generate significant amounts of classified information should be inspected at least annually. "Program needs," "degree of involvement," and "significant amounts" are not quantified, and components and subordinate commands have interpreted these phrases differently. For example, the Marine Corps performs self-inspections annually; the Naval Sea Systems Command performs self-inspections every 3 years; and Headquarters, Department of the Army, does not perform them. Navy and Army officials with whom we spoke cited resource constraints, and, in particular, staffing shortages, as the reason why inspections were not performed more often.

[19]Based on information provided by OUSD(I) for end of fiscal year 2003.

[20]The actual number of DOD personnel who completed an academy information security course in fiscal years 2003 and 2004 is less than 4,775 because some personnel completed multiple courses.

The DOD regulation's chapter on training requires DOD components to evaluate the quality and effectiveness of security training during self-inspections; however, none of the 19 components and subordinate commands we examined does so. Evaluating the quality of training during self-inspections can identify gaps in personnel's skill and competencies, and focus efforts to improve existing training.[21]

Ten of the 19 DOD components and subordinate commands we reviewed perform staff assistance visits of their lower echelon units in lieu of more rigorous self-inspections. Staff assistance visits, which typically are not staffed by inspectors, train the visited organization on how to meet inspection requirements, and any noted deficiencies are informally briefed to the local command staff. However, no official report is created for tracking and resolving deficiencies. According to ISOO officials, staff assistance visits do not fulfill the inspection requirement specified in Executive Order 12958, as amended. However, in commenting on a draft of this report, DOD officials stated that they were unaware of ISOO's position on staff assistance visits.

Of the 19 DOD components and subordinate commands we reviewed, only 7 conduct periodic document reviews as part of their self-inspections, although they are required to do so. In addition to revealing the types and extent of classification and marking errors, a document review can offer insight into the effectiveness of annual refresher training.

DOD Has Not Taken Sufficient Action to Ensure That Derivative Classification Decisions Are Based on Current Documentation

DOD has no assurance that personnel who derivatively classify information are using up-to-date security classification guides; however, our review showed that more than half of the estimated number of guides at the 17 organizations that could identify the number of guides they had were tracked for currency and updated at least every 5 years. DOD's approach to providing personnel access to up-to-date classification guides through a central library at its Defense Technical Information Center has been ineffective. OUSD(I) is studying ways to improve the centralized availability of up-to-date classification guides.

Executive Order 12958, as amended, directs agencies with original classification authority, such as DOD, to prepare security classification

[21] *GAO Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: Mar. 1, 2004).

guides to facilitate accurate and consistent derivative classification decisions. Security classification guides identify what information needs protection and the level of classification; the reason for classification, to include citing the applicable categories in the Executive Order; and the duration of classification. The ISOO directive and DOD regulation also require agencies to review their classification guides for currency and accuracy at least once every 5 years, and to update them as necessary. As table 3 shows, some DOD components and subordinate commands did not manage their classification guides to facilitate accurate derivative classification decisions. Since 2 of the 19 organizations were unable to provide us with the number of classification guides that they are responsible for, we could not determine the total number of classification guides belonging to the components and subordinate commands we reviewed. However, the remaining 17 organizations estimated their combined total to be 2,243 classification guides.

Table 3: Tracking of Security Classification Guides Varies among DOD Components

DOD component and subordinate commands	Estimated number of guides	Process to track guides
Army	Unknown	Not tracked at this organizational level.
Intelligence and Security Command	3	Currency of guides is tracked centrally. Centralized library has paper and electronic copies.
Army Materiel Command	Unknown	Not tracked at this organizational level.
Research, Development, and Engineering Command	65	Currency of guides is tracked centrally in an automated database. Some guides are available online to authorized users.
Navy/Marine Corps[a]	1,100	Centralized library has a paper copy of each guide. Currency of guides is not tracked centrally. Automated database is under development.
Naval Sea Systems Command	300	Centralized library has a paper copy of each guide. Currency of guides is not tracked centrally. Automated database is under development.
Naval Surface Warfare Center, Dahlgren Division	0	Not applicable.
Naval Air Systems Command	200	Currency of guides is tracked centrally in an automated database. Centralized library has a paper copy of each guide.
Marine Forces, Atlantic	0	Not applicable.
Air Force	525	Effort to create electronic versions of guides that will allow authorized users' access is ongoing. Currency of guides is tracked centrally.
Air Combat Command	0	Not applicable.

DOD component and subordinate commands	Estimated number of guides	Process to track guides
Air Force Materiel Command	416	Centralized library has a paper copy of each guide. Guides are tracked centrally in an automated database. Currency of guides not tracked.
88th Air Base Wing	36	Currency of guides is tracked centrally in an automated database. Centralized library has a paper or electronic copy of each guide.
Central Command	1	Electronic version of guide available to authorized users. Currency of guide is tracked centrally.
Special Operations Command	30	Centralized library has a paper copy of each guide. Automated database is under development that will allow authorized users to access electronic version of guides. Currency of guides tracked centrally.
National Geospatial-Intelligence Agency	10	Currency of guides is tracked, many of which are program specific and require less frequent updating.
Defense Intelligence Agency	9	Currency of guides is tracked centrally. Plan is to create electronic version of each guide for authorized users to access.
National Security Agency	500	Currency of guides is tracked centrally. Paper index of guides maintained.

Source: GAO analysis.

[a]Marine Corps security classification guides are managed by the Navy.

Of the 13 components and subordinate commands we reviewed that possess multiple classification guides:

- 10 maintain paper or electronic copies of classification guides in a central location, or are in the process of doing so;
- 8 track the currency of more than half of their combined classification guides to facilitate their review, to ensure that they are updated at least every 5 years, in accordance with the ISOO directive; and
- 8 either have made or are in the process of making their classification guides available to authorized users electronically. These 8 components and subordinate commands represent over 1,700—more than 75 percent—of the classification guides belonging to the DOD organizations that we reviewed.

DOD's strategy for providing personnel ready access to up-to-date security classification guides to use in making derivative classification decisions has been ineffective for two reasons. Officials at some of the DOD components and subordinate commands we examined told us that they routinely submit copies of their classification guides to the Defense

Technical Information Center, as required, while others told us they do not.[22] However, because of the way in which the Defense Technical Information Center catalogs its classification guide holdings, center officials could not tell us the names and the number of classification guides it possesses or is missing. In addition, center officials told us that they cannot compel original classification authorities to submit updated versions of their classification guides or report a change in status, such as a classification guide's cancellation. When the center receives a new classification guide, it enters up to three independent search terms in an electronic database to create a security classification guide index. As of October 2005, the center had in excess of 4,000 index citations for an estimated 1,400 classification guides, which is considerably fewer than the estimated 2,234 classification guides that 17 of the 19 components and subordinate commands reported possessing.

The absence of a comprehensive central library of up-to-date classification guides increases the potential for misclassification, because DOD personnel may be relying on insufficient, outdated reference material to make derivative classification decisions. Navy and Air Force officials showed us evidence of classification guides that had not been reviewed in more than five years, as the ISOO directive and DOD regulation require. As table 3 shows, several components and subordinate commands have taken or are taking action to improve derivative classifiers' access to security classification guides; however, except for the Air Force, there is no coordination among these initiatives, and neither the Defense Technical Information Center nor the OUSD(I) is involved. During our review, OUSD(I) officials told us that the department is studying how to improve its current approach to making up-to-date classification guides readily available, departmentwide.

[22]Section C2.5.3.4 of DOD 5200.1-R, *Information Security Program*, January 1997 requires original classification authorities to submit two copies of each approved security classification guide to the center, except for guides containing highly sensitive information. According to DOD declassification officials, less than 5 percent of the department's classification guides are classified at the Top Secret level, or contain Sensitive Compartmented Information or Special Access Program information.

Results of OSD Document Review Show Some Questionable Classification Decisions and Numerous Marking Errors

In our review of a nonprobability sample of 111 classified OSD documents we questioned DOD officials' classification decisions for 29 documents—that is, 26 percent of the sample. We also found that 93 of the 111 documents we examined (84 percent) had at least one marking error, and about half had multiple marking errors. Executive Order 12958, as amended, lists criteria for what information can be classified, and for markings that are required to be placed on classified records. While the results from this review cannot be generalized across DOD, they are indications of the lack of oversight and inconsistency that we found in DOD's implementation of its information security program.

To determine the extent to which personnel in five OSD offices followed established procedures for classifying information, we reviewed 111 documents recently classified by OSD, which revealed several questionable classification decisions and a large number of marking errors. In all, we questioned the classification decisions in 29, comprising 26 percent of the documents in the OSD sample. The majority of our questions pertained to whether all of the information marked as classified met established criteria for classification (16 occurrences), the seemingly inconsistent treatment of similar information within the same document (10 occurrences), and the apparent mismatch between the reason for classification and the document's content (5 occurrences). We gave the OSD offices that classified the documents an opportunity to respond to our questions, and we received written responses from the Offices of the Under Secretaries of Defense for Policy; Comptroller/Chief Financial Officer; and for Acquisition, Technology, and Logistics; regarding 17 of the 29 documents. In general, they agreed that several of the documents in question contained errors of misclassification. For example, we questioned the need to classify all of the information marked Confidential or Secret in 13 of the 17 documents. In their written responses, the three OSD offices agreed that, in 5 of the 13 documents, the information was unclassified, and in a sixth document the information should be downgraded from Secret to Confidential. The OSD offices did not state an opinion on 3 documents. We did not receive responses to our questions from the other two OSD offices on the remaining 12 documents.

The Executive Order, ISOO directive, and DOD's regulation together establish criteria for the markings that are required on classified records (see table 4).

Table 4: Required Markings on Classified Records

Marking requirement	Originally classified record	Derivatively classified record
Overall classification level of record cited	x	x
Portion markings present	x	x
"Declassify on" line completed	x	x
"Classified by" line completed	x	
Executive Order authorized "reason for" classification cited	x	
"Derived from" line completed		x

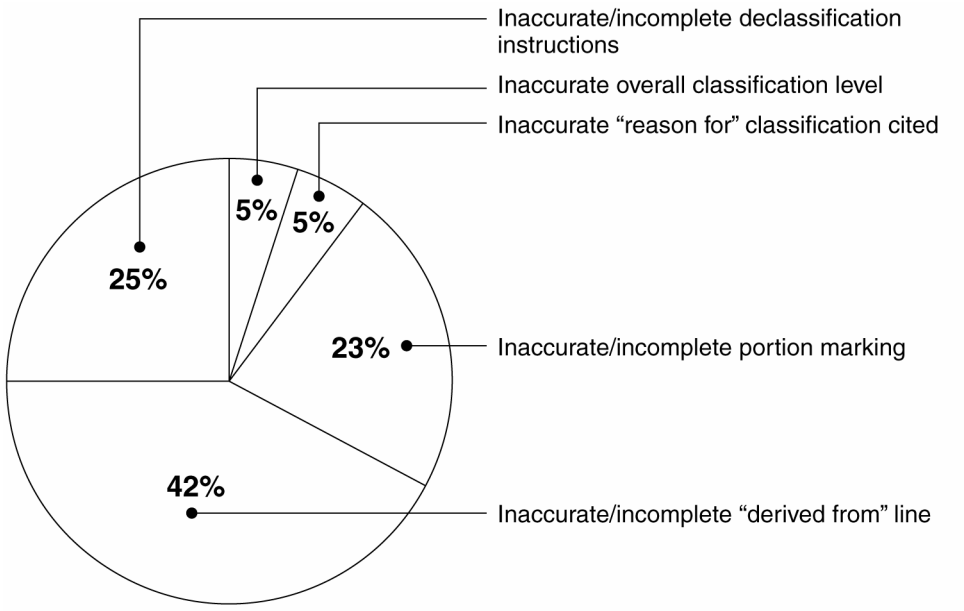
Source: GAO analysis.

The documents included in our document review were created after September 22, 2003, which is the effective date of ISOO's *Classified National Security Information Directive No. 1* and almost 6 months after Executive Order 12958 was last amended. The ISOO directive prescribes a standardized format for marking classified information that, according to the directive, is binding except in extraordinary circumstances or as approved by the ISOO Director.[23] To implement classification marking changes that resulted from the Executive Order and directive, DOD issued its own interim guidance on April 16, 2004.

Our review revealed that 93 of the 111 OSD documents (84 percent) had at least one marking error and about half of the documents had multiple marking errors, resulting in 1.9 errors per document we reviewed. As figure 2 shows, the marking errors that occurred most frequently pertained to declassification, the sources used in derivative classification decisions, and portion marking.

[23]32 C.F.R. §2001.20 (2003).

Figure 2: Distribution of Marking Errors Detected in OSD Document Sample (n = 213 errors)



Source: GAO analysis.

The most common marking errors that we found in the OSD document sample, by type of marking error, are listed in table 5.

Table 5: Examples of Common Marking Errors in OSD Document Sample

Types of marking errors	Examples of marking errors
Inaccurate or incomplete declassification instructions	• source not provided; therefore, unable to determine • discontinued exemption codes • formerly restricted data exempt • originating agency's determination required
Inaccurate or incomplete "derived from" line	• title of source document omitted • date of source document omitted • "classified by" line incorrectly inserted
Inaccurate or incomplete portion marking	• entire pages not marked • individual paragraphs not marked • section titles not marked • subject line not marked
Inaccurate "reason for" classification cited	• section 1.6., not section 1.4. of Executive Order cited • section 1.6. without a subsection cited

Types of marking errors	Examples of marking errors
Inaccurate overall classification level	• not releasable to foreign nationals caveat not included in portion markings • releasable to the United States of America, Canada, and the United Kingdom caveat present in portion marking, but not included in page marking

Source: GAO analysis.

Since ISOO issued its directive in September 2003, it has completed 19 classified document reviews of DOD components and subordinate commands.[24] The types of marking errors that ISOO reported finding were similar to what we found among the OSD documents. Specifically, marking errors associated with declassification, source, and portion marking represented more than 60 percent of the errors in both document samples.

The Accuracy of DOD's Classification Decisions Estimate Is Questionable

DOD's estimate of how many classification decisions it makes each year is of questionable accuracy. Although ISOO provides DOD components with guidance as to how they should calculate classification decisions, we found considerable variance within the department in how this guidance was implemented. For example, there was inconsistency regarding which records are included in the estimate, the number and types of lower echelon units that are included, when to estimate, and for how long to estimate.

ISOO requires federal agencies to estimate the number of original and derivative classification decisions they made during the previous fiscal year, which ISOO includes in its annual report to the President. Agency estimates are based on counting the number of Confidential, Secret, and Top Secret original and derivative classification decisions during a designated time period and extrapolating an annual rate from them. According to ISOO guidance, agencies typically count their classification decisions during a consecutive 2-week period in each of the four quarters of the fiscal year, for a combined total of 8 weeks.

OUSD(I) officials told us that two highly classified categories of information, sensitive compartmented information and special access programs, are included in the count; however, several components and

[24]The five OSD offices that participated in our document review did not participate in any of the ISOO document reviews.

subordinate commands we examined omit these categories from their totals. In addition, some components and subordinate commands—such as the Army's Research, Development, and Engineering Command and the National Geospatial-Intelligence Agency—include e-mails in their count, while others—such as the Defense Intelligence Agency and the Central Command—do not. Whether or not to include e-mails can dramatically affect counts. For example, the National Security Agency's classification estimate declined from 12.5 million in fiscal year 2002 to only 7 in fiscal year 2003. Agency officials attributed this dramatic drop to e-mails being included in the totals for fiscal year 2002 and not for fiscal year 2003.

Some DOD components and subordinate commands do not query their entire organization, to encompass all personnel who may be classifying information. For example, the Defense Intelligence Agency randomly selects four of its eight directorates to participate, and the National Security Agency and the Naval Air Systems Command selects only lower echelon organizations that have an original classification authority. As a result, these locations omit an unknown number of derivative classification decisions. The Navy bases its annual estimate on data covering a 2-week period from each of its major commands once per year rather than from all of its commands, four times per year as suggested in ISOO guidance. For example, during the first quarter, the Marine Corps is queried, and during the second quarter, the fleet commands are queried. Also, some of the combatant commands' service components are not queried at all, such as the Army's component to the European Command, the Navy's component to the Transportation Command, the Air Force's component to the Southern Command, and the Marine Corps' component to the Central Command. In commenting on a draft of this report, the department correctly points out that guidance issued by ISOO allows each component to decide who to include in its classification decisions estimate.

The Special Operations Command and the Central Command both schedule their counts at the end of the fiscal year; 4 consecutive weeks at the former, and 8 consecutive weeks at the latter. Special Operations Command officials told us that the end of the fiscal year tends to be a slower operational period, thereby allowing more time to conduct the data collection.

DOD components and subordinate commands convert their estimates in different ways to project an entire year. Those that conform to the suggested ISOO format of four 2-week counting periods a year (that is, 8 weeks) multiply their counts by 6.5 (that is, 8 weeks x 6.5 = 52 weeks). The

Navy, however, multiplies each of its four separate counts by 429 to account for all of the lower echelon units not represented in the estimate.[25]

Our review of DOD's submissions to ISOO of its estimated number of classification decisions for fiscal years 2000 through 2004, revealed several anomalies. For example, the National Reconnaissance Office reported making more than 6 million derivative and zero original classification decisions during this 5-year period, and the Marine Forces, Atlantic, reported zero derivative and zero original classification decisions during fiscal years 2003 and 2004. Subsequent conversations with Marine Forces, Atlantic, officials indicated that a misunderstanding as to what constitutes a derivative classification decision resulted in an underreporting for those 2 years.

Other examples of DOD component data submissions during this 5-year time period that had either a disproportionate reporting of original versus derivative classification decisions or a significant change in counts from 1 year to the next include:

- DOD reported in fiscal year 2004 that, departmentwide, about 4 percent of its classification decisions were original, yet the Defense Advanced Research Projects Agency and the Joint Forces Command both reported that more than 70 percent of their classification decisions were original.

- DOD reported in fiscal year 2003, that departmentwide, less than 2 percent of its classification decisions were original, yet the Joint Staff and the European Command both reported more than 50 percent of their classification decisions were original.

- DOD reported in fiscal year 2002 that, departmentwide, less than 1 percent of its classification decisions were original, yet the Office of the Secretary of Defense and the Southern Command both reported more than 20 percent of their classification decisions were original.

- DOD reported an increase in the number of original classification decisions during the fiscal year 2002 through 2004 period, from 37,320

[25]429 is derived from the formula 26 x 33 ÷ 2 = 429, where 26 represents the number of 2-week counting periods in a year, 33 is a multiplier to account for those commands among the Navy's 3,960 commands that are not counted, and 2 is a divisor to account for those commands that have no classification activity, such as dental clinics and commissaries.

to 47,238 (about a 27 percent increase), to 198,354 (about a 300 percent increase). However, during this same 3-year period, the Navy's trend for original classification decisions was from 1,628 to 16,938 (about a 900 percent increase) to 1,898 (about a 90 percent decrease); and the Army's trend was from 10,417 to 2,056 (about an 80 percent decrease) to 133,791 (about a 6,400 percent increase).

DOD reported a 75 percent decrease in the total number of classification decisions (that is, original and derivative) from fiscal year 2002 to fiscal year 2004, yet several DOD components reported a significant increase in overall classification decisions during this same time period, including the Defense Threat Reduction Agency (a 20,107 percent increase), the Southern Command (1,998 percent increase), Defense Intelligence Agency (a 1,202 percent increase), and the National Geospatial-Intelligence Agency (a 354 percent increase).

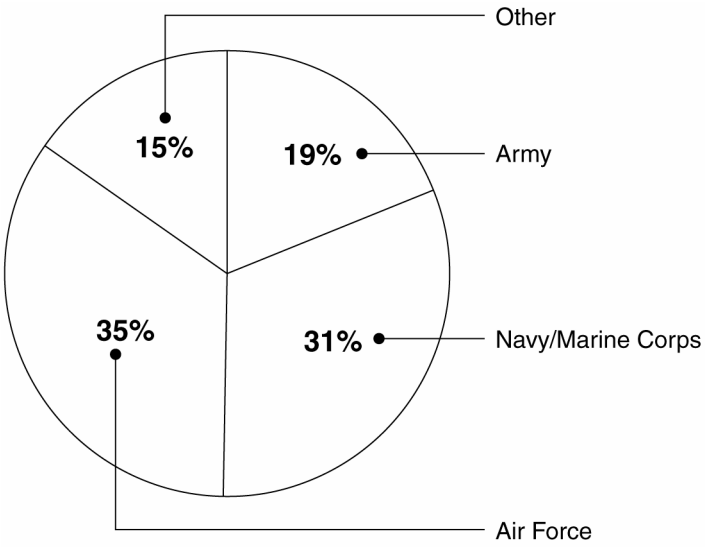
OUSD(I) has decided to discontinue the practice of DOD components submitting their classification decisions estimates directly to ISOO. Beginning with the fiscal year 2005 estimates, OUSD(I) will scrutinize the classification decision estimates of its components before consolidating and submitting them to ISOO. Properly conducted, OUSD(I)'s review could improve the accuracy of these estimates, if methodological inconsistencies are reduced.

DOD's Ability to Meet All of the Executive Order's Automatic Declassification Deadlines Depends on the Actions of Other Federal Agencies

Army, Navy, and Air Force classification officials told us that the military services are on pace to meet the target date of 2006 for reviewing their own classified documents that qualify for automatic declassification, and for referring records that contain classified information belonging to other agencies to those agencies—an assertion endorsed by ISOO in its 2004 report to the President. However, these officials told us that they are less likely to meet the target date of 2009 for reviewing records referred to them, and of 2011 for reviewing special media (such as audio and video recordings). DOD's ability to satisfy the 2009 and 2011 target dates depends, to a great extent, on the actions of other federal agencies.

We limited our review of DOD's automatic declassification program to the four military services because, as figure 3 shows, they performed 85 percent of all the declassification within DOD in fiscal year 2004.

Figure 3: DOD Automatic Declassification Activity in Fiscal Year 2004, as Measured by the Number of Pages Declassified



Source: GAO's analysis of ISOO data.

Executive Order 12958, as amended, stipulates that on December 31, 2006, and on December 31 of every year thereafter, classified records that are (1) at least 25 years old and (2) of permanent historical value shall in general be automatically declassified, whether or not they have been reviewed. The Executive Order sets a record's date of origination as the time of original classification, and it also exempts certain types of information from automatic declassification, such as information related to the application of intelligence sources and methods. The automatic declassification deadline for records containing information classified by more than one agency, such as the Army and the Air Force or the Army and the Central Intelligence Agency, is December 31, 2009, and for special media it is December 31, 2011. For the most part, only the originating agency can declassify its own information. Consequently, if the Army discovers classified information that was originated by the U.S. State Department, the Army must alert the State Department and refer the information to the State Department for resolution. The Executive Order describes special media as microforms, motion pictures, audiotapes, videotapes, or comparable media that make its review for possible declassification exemptions "more difficult or costly."[26] The ISOO directive

[26]Executive Order 12958, as amended, §3.3.(e)(2).

mirrors these requirements and directs ISOO, in conjunction with its parent organization, the National Archives and Records Administration, and other concerned agencies to develop a standardized process for referring records containing information classified by more than one agency across the federal government.

Army, Navy/Marine Corps, and Air Force classification officials told us that they face a variety of challenges impacting their ability to meet the target dates of 2009 for reviewing records referred to them, and of 2011 for reviewing special media. Based on information provided by officials from the military services and the National Archives and Records Administration who are responsible for the automatic declassification effort, it appears that three obstacles hinder their progress toward meeting these deadlines. DOD's ability to remove these obstacles without the involvement of other federal agencies is limited. First, there is no federal government standard for annotating classified records that contain information classified by more than one agency. For example, two non-DOD agencies both annotate their records with a "D" and an "R," but for opposite purposes. That is, one of the agencies uses a "D" to denote "deny automatic declassification" and an "R" to denote "release," while the other agency uses a "D" to denote "declassify" and an "R" to denote "retain." The National Archives and Records Administration and various interagency working groups and task forces have sought a federal government standard, but National Archives officials told us that they were not optimistic that agencies would reach agreement soon. According to these officials, the lack of a federal government standard has contributed to the inadvertent release of classified information.

Second, there is no central location within DOD or the federal government for storing records eligible for automatic declassification that contain information classified by multiple DOD components or non-DOD agencies. To review records originated by the four military services, agencies must send personnel trained to evaluate information for declassification suitability to as many as 14 different sites where the records are stored. For example, the Air Force has records eligible for automatic declassification at storage sites located in Ohio, Alabama, and Texas (see figure 4). National Archives officials pointed out that consolidating the records at fewer sites may be more efficient, and likely more cost-effective.

Figure 4: Locations of Army, Navy, Air Force, and Marine Corps Automatic Declassification Sites

Sources: DOD; Copyright © Corel Corp. All rights reserved (map).

A third factor that may cause DOD to miss meeting the Executive Order deadlines is the lack of a common database that federal government agencies can use to track the status of records containing information classified by more than one agency. The ISOO directive allows federal government agencies to utilize electronic databases to notify other agencies of their referrals; however, agencies have created their own databases that operate independently of one another. In commenting on a draft of this report, DOD officials stated that, despite the lack of federal government standards, the department has been a leading proponent of

working collaboratively with other federal agencies to meet automatic declassification deadlines. We cannot confirm the accuracy of DOD's characterization because DOD's relationship with other agencies involved in automatic declassification was not part of our review.

Conclusions

The Under Secretary of Defense for Intelligence has delegated the execution and oversight of information security to the DOD component level. This decentralized approach, coupled with inconsistency in the implementation of components' information security programs, has resulted in wide variance in the quality of these programs. For example, the OUSD(I) does not directly monitor components' compliance with federal and DOD training, self-inspection, and documentation requirements stipulated in Executive Order 12958, as amended; the ISOO directive; and the DOD regulation. Inadequate classification management training, self-inspections, and security classification guide documentation among the various DOD components increase the risk of (1) poor classification decisions and marking errors, similar to what we observed in our OSD document review; (2) restricting access to information that does not pose a threat to national security; and (3) releasing information to the general public that should still be safeguarded.

OUSD(I) oversight could reduce the likelihood of classification errors. For example, if OUSD(I) ensured that components evaluated the quality and effectiveness of training and periodically included document reviews in their self-inspections, prevalent classification errors could be addressed through annual refresher training that derivative classifiers complete. Evaluating the quality of training can assist components in targeting scarce resources on coursework that promotes learning and reduces misclassification. Although the results of our review of a sample of OSD documents cannot be generalized departmentwide, we believe these results coupled with the weaknesses in training, self-inspections, and documentation that we found at numerous components and subordinate commands increases the likelihood that documents are not being classified in accordance with established procedures.

DOD's estimate of how many original and derivative classification decisions it makes annually is unreliable because it is based on data from the DOD components that were derived using different assumptions about what should be included and about data collection and estimating techniques. Still, this estimate is reported to the President and to the public, and it is routinely cited in congressional testimony by DOD officials and freedom of information advocates as authoritative. During

our review, OUSD(I) decided to resume its practice of reviewing components' classification estimates before they are submitted to ISOO. If properly implemented, this review could improve data reliability to some extent, but only if it addresses the underlying lack of uniformity in how the individual DOD components are collecting and manipulating their data to arrive at their estimates.

The automatic declassification provision in Executive Order 12958, as amended, requires agencies generally to declassify records that are 25 years old or more and that no longer require protection. The Army, Navy/Marine Corps, and Air Force reported they are on track to review all of the documents they classified before the deadline; however, they are less likely to complete their review of the untold number of records containing information classified by other DOD components and non-DOD agencies by the deadlines set in the Executive Order. As the deadlines pass and these records are automatically declassified, information that could still contain national security information becomes more vulnerable to disclosure. DOD's ability to meet these deadlines is jeopardized both by conditions beyond and conditions within its direct control. For example, DOD cannot require non-DOD agencies to adopt a national standard for annotating classified records, but it can take action to streamline the process of reviewing records containing information classified by more than one DOD component.

Recommendations for Executive Action

To reduce the risk of misclassification and create greater accountability across the department, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to

- establish a centralized oversight process for monitoring components' information security programs to ensure that they satisfy federal and DOD requirements. This oversight could include requiring components to report on the results of self-inspections or other actions, targeted document reviews, and/or reviews by the DOD Inspector General and component audit agencies.

- to issue a revised *Information Security Program* regulation to ensure that

    - those personnel who are authorized to and who actually perform classification actions, receive training that covers the fundamental classification principles as defined in the Under Secretary's memorandum of November 30, 2004 and that completion of such

training is a prerequisite for these personnel to exercise this authority;

- the frequency, applicability, and coverage of self-inspections, and the reporting of inspection results are based on explicit criteria; and
- authorized individuals can access up-to-date security classification guides necessary to derivatively classify information accurately.

To support informed decision making with regard to information security, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to institute quality assurance measures to ensure that components implement consistently the DOD guidance on estimating the number of classification decisions, thereby increasing the accuracy and reliability of these estimates.

To assist DOD in its efforts to meet automatic declassification deadlines, we recommend that the Secretary of Defense direct the Under Secretary of Defense for Intelligence to evaluate the merits of consolidating records eligible for automatic declassification that contain information classified by multiple DOD components at fewer than the current 14 geographically dispersed sites.

Agency Comments and Our Evaluation

In commenting on a draft of this report, DOD concurred with all six recommendations; however, the department expressed concern that we did not accurately portray the Navy's program for managing its security classification guides. Upon further review, we modified table 3 in the report and accompanying narrative to indicate that the Navy (1) does have a centralized library containing paper copies of its security classification guides, and (2) is developing an automated database to make its classification guides available to authorized users electronically. We disagree with the department's assertion that the Navy is tracking its classification guides to ensure that they are reviewed at least once every 5 years for currency and are updated accordingly. Based on our discussions with Navy information security officials, including the Retrieval and Analysis of Navy (K)lassified Information (RANKIN) Program Manager, and observing a demonstration of the spreadsheet used to catalog security classification guide holdings, we saw no evidence to suggest that currency of guides is being systematically tracked. With respect to our fifth recommendation that focuses on how DOD estimates the number of classification decisions it makes each year, we endorsed the department's decision to continue scrutinizing its components' estimates before

consolidating and submitting them to ISOO. However, we continue to believe that OUSD(I) should augment its after-the-fact review with measures to ensure that components follow a similar process to derive their classification decisions estimates, such as standardizing the types of records to be included. Adopting a consistent methodology across the department and from year to year should improve the reliability and accuracy of this estimate that is reported to the President.

DOD also provided technical comments for our consideration in the final report, which we incorporated as appropriate. DOD's formal comments are reprinted in appendix II.

We are sending copies of this report to the Secretaries of Defense, the Army, the Navy, and the Air Force; the Commandant of the Marine Corps; and the Directors of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Security Agency. 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) 512-5431 or dagostinod@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,

Davi M. D'Agostino
Director, Defense Capabilities and
Management

Appendix I: Scope and Methodology

To conduct our review of the Department of Defense's (DOD's) information security program, we met with officials and obtained relevant documentation from the following DOD components and subordinate commands:

- Department of the Army, Office of the Deputy Chief of Staff for Intelligence, Arlington, Virginia;
  - U.S. Army Intelligence and Security Command, Fort Belvoir, Virginia;
  - U.S. Army Materiel Command, Fort Belvoir, Virginia;
  - U.S. Army Research, Development and Engineering Command, Aberdeen Proving Ground, Maryland;
- Department of the Navy, Office of the Chief of Naval Operations, Arlington, Virginia;
  - Naval Sea Systems Command, Washington, D.C.;
  - Naval Surface Warfare Center Dahlgren Division, Dahlgren, Virginia;
  - Naval Air Systems Command, Patuxent River, Maryland;
- Department of the Air Force Air and Space Operations, Directorate of Security Forces, Information Security Division, Rosslyn, Virginia;
  - Air Force Air Combat Command, Langley Air Force Base, Virginia;
  - Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio;
  - 88th Security Forces Squadron, Wright-Patterson Air Force Base, Ohio;
- Headquarters, U.S. Marine Corps, Arlington, Virginia;
  - U.S. Marine Forces, Atlantic, Norfolk Naval Base, Virginia;
- Headquarters, U.S. Central Command, MacDill Air Force Base, Florida;
- Headquarters, U.S. Special Operations Command, MacDill Air Force Base, Florida;
- National Geospatial-Intelligence Agency, multiple sites in the Washington, D.C. metropolitan area;
- Defense Intelligence Agency, Washington, D.C.;
- National Security Agency, Fort Meade, Maryland; and
- Headquarters, Defense Technical Information Center, Fort Belvoir, Virginia.

The information security programs of these nine components, collectively, were responsible for about 83 percent of the department's classification decisions each of the last 3 fiscal years that data are available (2002 through 2004). We selected the information security programs of three Army, three Navy, three Air Force, and one Marine Corps subordinate command because they had among the largest number of classification decisions for their component during the fiscal year 2002 through 2004 time period.

To examine whether DOD's implementation of its information security management program in the areas of training, self-inspections, and security classification guide management effectively minimizes the risk of misclassification, we compared the DOD components' and subordinate commands' policies and practices with federal and DOD requirements, including Executive Order 12958, *Classified National Security Information*, as amended; Information Security Oversight Office (ISOO) Directive 1, *Classified National Security Information;* and DOD *Information Security Program* regulation 5200.1-R. Additionally, we visited the Defense Security Service Academy in Linthicum, Maryland, to discuss DOD training issues, and the Defense Technical Information Center at Fort Belvoir, Virginia, to discuss the availability of current security classification guides. We also met with officials from the Congressional Research Service, the Federation of American Scientists, and the National Classification Management Society to obtain their perspectives on DOD's information security program and on misclassification of information in general.

To assess the extent to which DOD personnel in five offices of the Office of the Secretary of Defense (OSD) followed established procedures for classifying information, to include correctly marking classified information, we examined 111 documents classified from September 22, 2003 to June 30, 2005. Because the total number of classified documents held by DOD is unknown, we could not pursue a probability sampling methodology to produce results that could be generalized to either OSD or DOD. The September 22, 2003 start date was selected because it coincides with when the ISOO directive that implements the Executive Order went into effect. OSD was selected among the DOD components because it has been the recipient of fewer ISOO inspections than most of the other DOD components, and we expected comparatively greater compliance with the Executive Order since DOD's implementing regulation, DOD 5200.1-R, was published by an OSD office. We selected the following five OSD offices located in Washington, D.C. to sample:

- Office of the Director of Program Analysis and Evaluation;
- Office of the Under Secretary of Defense for Policy;
- Office of the Under Secretary of Defense for Acquisition, Technology and Logistics;
- Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer; and
- Office of the Under Secretary of Defense Comptroller/Chief Financial Officer.

These five offices were responsible for 84 percent of OSD's reported classification decisions (original and derivative combined) during fiscal year 2004. According to the Pentagon Force Protection Agency, the office responsible for collecting data on classification activity for OSD, we obtained 100 percent of these five office's classification decisions during the 21-month time period. Two GAO analysts independently reviewed each document using a 16-item checklist that we developed based on information in the Executive Order, and feedback from ISOO classification management experts. [1] GAO analysts who participated in the document review completed the Defense Security Service Academy's online *Marking Classified Information* course and passed the embedded proficiency test.

Each document was examined for compliance with classification procedures and marking requirements in the Executive Order. The two analysts' responses matched in more than 90 percent of the checklist items. On those infrequent occasions where the analysts' responses were dissimilar, a third GAO analyst conducted a final review. We examined the rationale cited by the classifier for classifying the information, and whether similar information within the same document and across multiple documents was marked in the same manner. We also performed Internet searches on official U.S. Government Web sites to determine if the information had been treated as unclassified. For those documents that we identified as containing questionable classification decisions, we met with security officials from the applicable OSD offices to obtain additional information and documentation.

To assess the reliability of DOD's annual classification decisions estimate and the existence of material inconsistencies, we compared the guidance issued by ISOO and the Office of the Under Secretary of Defense for Intelligence on methods to derive this estimate with how DOD components and subordinate commands implemented this guidance. We also scrutinized the data to look for substantial changes in the data estimates reported by DOD components during fiscal years 2002 through 2004.

To determine the likelihood of DOD's meeting automatic declassification deadlines contained in Executive Order 12958, as amended, we met with officials from the Army, Navy/Marine Corps, and Air Force declassification

[1] 12 of the 16 checklist items applied to originally classified documents, and 13 of the 16 checklist items applied to derivatively classified documents.

offices. We decided to focus exclusively on the four military services, because, collectively they were responsible for more than 85 percent of the department's declassification activity during fiscal year 2004. We also met with ISOO officials to discuss their evaluation of DOD's progress towards meeting the Executive Order deadlines. To increase our understanding of the impediments that federal agencies in general, and DOD in particular, face with regard to satisfying automatic declassification deadlines, we met with declassification officials from the National Archives and Records Administration in College Park, Maryland.

We met with ISOO officials to discuss the assignment's objectives and methodology, and received documents on relevant information security topics, including inspection reports.

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

Appendix II: Comments from the Department of Defense

INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

JUN 12 2006

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino,

Enclosed is the Department of Defense (DoD) response to the GAO draft report, "MANAGING SENSITIVE INFORMATION: DoD Can More Effectively Reduce the Risk of Classification Errors," dated May 11, 2006, (GAO Code 350684/GAO-06-706).

The Department concurs with the GAO recommendations and has provided comments pertaining to the technical aspects discussed in the report.

We appreciate the courtesies extended by your staff during this audit and their willingness to work with the Department on these matters. If you have any questions, please contact Mrs. Debbie Ross, Acting Deputy Director for Information Security Policy, at 703-571-0261.

Sincerely,

Robert Andrews 12/06/06

Robert Andrews
Deputy Under Secretary of Defense
(Counterintelligence and Security)

Enclosure:
As stated

cc:
DoD OIG

GAO DRAFT REPORT – DATED MAY 11, 2006
GAO CODE 350684/GAO-06-706

"MANAGING SENSITIVE INFORMATION: DoD Can More Effectively Reduce the Risk of Classification Errors"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: We recommend the Secretary of Defense direct the Under Secretary of Defense for Intelligence to establish a centralized oversight process for monitoring components' information security programs to ensure that they satisfy federal and DoD requirements. This oversight could include requiring components to report on the results of self-inspections or other actions, targeted document reviews, and/or reviews by the DoD Inspector General and component audit agencies.

DOD RESPONSE: Concur based on the findings of the GAO audit and the Department's own observations on these matters when accompanying the Information Security Oversight Office on oversight visits to some of the Defense components.

RECOMMENDATIONS 2-4: We recommend the Secretary of Defense direct the Under Secretary of Defense for Intelligence to issue a revised Information Security Program regulation to ensure that

- Those personnel who are authorized to and who actually perform classification actions, receive training that covers the fundamental classification principles as defined in the Under Secretary's memorandum of November 30, 2004 and that completion of such training is a prerequisite for these personnel to exercise this authority;
- The frequency, applicability, and coverage of self-inspections, and the reporting of inspection results are based on explicit criteria; and,
- Authorized individuals can access up-to-date security classification guides necessary to derivatively classify information accurately.

DOD RESPONSE: Concur. The Department has a requirement for all classifiers to receive training prior to exercising classification authority. However, we are concerned that the report does not accurately portray the overall Navy program for managing security classification guidance. The report only indicates the results of how some Department of Navy (DON) commands maintain their Security Classification Guides (SCGs). It does not address the DON's centralized repository of SCGs, which is maintained by the Chief of Naval Operations (CNO (N09N2)), Retrieval and Analysis of Navy (K)lassified Information (RANKIN) Program Manager. The RANKIN Program

Manager also tracks SCGs for currency. Technical accuracy is the responsibility of the Original Classification Authority (OCA). The DON issues SCGs via the OPNAVINST 5513 series. This program was described in detail to the GAO Auditor team, by the RANKIN Program Manager and the recently departed CNO (N09N2), Information Security Policy Branch Head, yet there is no mention of it in the report. Also, the RANKIN Program Manager is working on an automated solution, to post the DON's SCGs on a secure network. This site will be restricted to those personnel with a valid need-to-know, and will be centrally managed by the RANKIN Program Manager. The benefit of automating the SCGs is to reduce the amount of time spent by derivative classifiers to obtain current SCGs, better facilitate currency of SCGs via the OCA, increase protection of information, and aid derivative classifiers in the proper classification of information. It is appropriate and necessary to include this information in the report as well.

RECOMMENDATION 5: We recommend the Secretary of Defense direct the Under Secretary of Defense for Intelligence to institute quality assurance measures to ensure that components implement the DoD guidance consistently, thereby increasing the accuracy and reliability of these estimates.

DOD RESPONSE: Concur. The Department is already doing it with this iteration of data collection.

RECOMMENDATION 6: We recommend the Secretary of Defense direct the Under Secretary of Defense for Intelligence to evaluate the merits of consolidating records eligible for automatic declassification that contain information classified by multiple DoD components at fewer than the current 14 geographically dispersed sites.

DOD RESPONSE: Concur. The Department has advised the Information Security Oversight Office that we agree with this concept in theory at the national level. Also, the Military Departments are looking into the feasibility of setting up a DoD Declassification Referral Center to facilitate declassification reviews of records containing multiple DoD component equities.

TECHNICAL COMMENTS

GAO Highlights Page, 3rd Para. Replace everything after the first line with "of the considerable variance in how ISOO's guidance is implemented across the Department, and from year to year. Since 2002, responsibility for monitoring and assessing DoD component's data submission has passed between DoD and ISOO. OUSD(I) resumed consolidating the DoD response in 2005 to aid in identifying potential oversight issues. *Reason:* Provides correct background on this issue. Also, the data is not used by DoD to

make resource decisions because DoD does not think the report provides sufficient information to do so.

Page 6, 2nd Para, 3rd Sentence. Delete 3rd sentence and replace everything after the 5th sentence with "However, it has been DoD's practice to implement ISOO's guidance which allows each DoD component to determine who they should sample within their organization. This was also ISOO's practice when they were collecting data direct from DoD components during Fiscal Years 2002-2004. In fiscal year 2005, OUSD(I) resumed responsibility for scrutinizing the estimates of its components before consolidating and submitting them to ISOO for inclusion in its annual report to the President. *Reason:* Correctness.

Page 7, 1st Para, 2nd Sentence. Add before last sentence, "It was noted that DoD has been one of the leading proponents in working collaboratively with other federal agencies to facilitate this process inspite of the lack of federal standards." Reason: Correct.

Page 16, 1st Para, Last 2 Sentences. Delete. *Reason:* This information is irrelevant since these DoD components have their own training which may be just as adequate as the DSSA training.

Page 20, Table 3, Last Column. For the Naval Sea Systems Command entry, change to "Currency of guides tracked centrally. Centralized paper index of paper guides maintained. Automated database being implemented by CNO." *Reason:* While they may be behind in tracking the guides, they still have a system in place for central tracking and are working to get it current.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino (202) 512-5431 or dagostinod@gao.gov.

Acknowledgments

Ann Borseth, Mattias Fenton, Adam Hatton, Barbara Hills, David Keefer, David Mayfield, Jim Reid, Terry Richardson, Marc Schwartz, Cheryl Weissman, and Jena Whitley 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