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

March 2006

MANAGING SENSITIVE INFORMATION

Departments of Energy and Defense Policies and Oversight Could Be Improved

GAO-06-369

March 2006

MANAGING SENSITIVE INFORMATION

Departments of Energy and Defense Policies and Oversight Could Be Improved

GAO Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

What GAO Recommends

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

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

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

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

What GAO Found

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

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

Contents

Letter 1

Results in Brief 3
DOE and DOD Lack Clear OUO and FOUO Guidance in Key Aspects 4
Neither DOE nor DOD Requires Training or Conducts Oversight 9
Conclusions 11
Recommendations for Executive Action 12
Agency Comments and Our Evaluation 12

Appendix I **Comments from the Department of Energy** 16

Appendix II **Comments from the Department of Defense** 20

Appendix III **GAO Contacts and Staff Acknowledgments** 23

Table

Table 1: FOIA Exemptions 5

Figure

Figure 1: DOE's OUO Stamp 7

Abbreviations

DOD Department of Defense
DOE Department of Energy
FOIA Freedom of Information Act
FOUO For Official Use Only
OUO Official Use Only

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 7, 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:

In the interest of protecting national security, the federal government routinely classifies certain documents and other information as Top Secret, Secret, or Confidential. In addition to classified information, federal agencies also place dissemination restrictions on unclassified but sensitive information. These restrictions are used to indicate that the information, if disseminated to the public or persons who do not need such information to perform their jobs, may cause foreseeable harm to protected governmental, commercial, or privacy interests. Such information includes, for example, sensitive personnel information, such as Social Security numbers, and the floor plans for some federal buildings. The Department of Energy (DOE) and the Department of Defense (DOD) use the designations Official Use Only (OUO) and For Official Use Only (FOUO), respectively, to identify information that is unclassified but sensitive. According to both DOE and DOD officials, it is unknown how many documents containing OUO and FOUO information exist, but a DOE official stated that there were many millions of pages of OUO material. Congressional concern has recently arisen that some government officials may be improperly designating certain documents as unclassified but sensitive, which unnecessarily limits their dissemination to the public.

DOE's and DOD's OUO and FOUO programs are largely based on the exemption provisions of the Freedom of Information Act (FOIA), which establishes the public's legal right of access to government information, as well as the government's right to restrict public access to certain types of unclassified information.[1] FOIA identifies nine categories of information that are generally exempt from public release, including law enforcement

[1]Freedom of Information Act (5 U.S.C. § 552).

records and proprietary information, although only eight of these categories are applicable to OUO and FOUO programs.[2]

This report responds in part to your request that we review the broad issues regarding information classification management at DOE and DOD. As agreed with your office, to respond to your request, we will issue three reports on this subject. This report discusses OUO and FOUO programs at DOE and DOD. In addition, in June 2006, we will issue two separate reports on DOE's and DOD's management of information classified as Top Secret, Secret, or Confidential, which is separate from the agencies' OUO and FOUO programs. In this report, we will (1) identify and assess the policies, procedures, and criteria DOE and DOD employ to manage OUO and FOUO information and (2) determine the extent to which DOE's and DOD's training and oversight programs assure that information is identified, marked, and protected according to established criteria.

We also recently issued a report on the designation of sensitive security information at the Transportation Security Administration.[3] Finally, we are currently reviewing the management of Sensitive but Unclassified information within the Department of Justice, the agency's current efforts to share sensitive homeland security information among federal and nonfederal entities, and the challenges posed by such information sharing.

To identify and assess the policies and procedures DOE and DOD use to manage OUO and FOUO information, we reviewed and analyzed FOIA and DOE's and DOD's current applicable policies, regulations, orders, manuals, and guides. We compared these to the objectives and fundamental concepts of internal controls defined in *Standards for Internal Control in the Federal Government*.[4] To determine the extent to which these agencies' internal controls assure that information is identified and

[2]FOIA exemption 1 solely concerns classified information, which is governed by Executive Order; DOE and DOD do not include this category in their OUO and FOUO programs since the information is already restricted by each agency's classified information procedures. In addition, exemption 3 addresses information specifically exempted from disclosure by statute, which may or may not be considered OUO or FOUO. Information that is classified or controlled under a statute, such as Restricted Data or Formerly Restricted Data under the Atomic Energy Act, is not also designated as OUO or FOUO.

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

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

marked according to established criteria, we reviewed the training provided to staff at both agencies and the oversight conducted on the OUO and FOUO programs. We compared these efforts with the standards for training and oversight envisioned in *Standards for Internal Control in the Federal Government*. We also interviewed officials from DOE and DOD in Washington, D.C.; at DOE field locations in Los Alamos and Albuquerque, New Mexico, Oak Ridge, Tennessee, and the Savannah River Site in South Carolina; and at several DOD field locations. These locations were selected based on the large amounts of activity in classifying and controlling information. According to agency officials, there is no listing or identifiable universe of OUO or FOUO documents maintained by the agencies. Because of this limitation, we did not sample documents marked OUO or FOUO.

We performed our work from April 2005 through January 2006 in accordance with generally accepted government auditing standards.

Results in Brief

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

While both DOE and DOD offer training on their OUO and FOUO policies, neither DOE nor DOD has an agencywide requirement that employees be trained before they designate documents as OUO or FOUO. Moreover,

neither agency conducts oversight to assure that information is appropriately identified and marked as OUO or FOUO. According to *Standards for Internal Control in the Federal Government*, training and oversight are important elements in creating a good internal control program. DOE and DOD officials told us that limited resources, and in the case of DOE, the newness of the program, have contributed to the lack of training requirements and oversight. Nonetheless, the lack of training requirements and oversight of the OUO and FOUO programs leaves DOE and DOD officials unable to assure that OUO and FOUO documents are marked and handled in a manner consistent with agency policies and may result in inconsistencies and errors in the application of the programs.

We are recommending that DOE and DOD clarify their policies to assure the consistent application of OUO and FOUO designations and increase the level of management oversight in their use. In commenting on a draft of this report, DOE and DOD agreed with most of our recommendations. Both DOE and DOD disagreed with our recommendation to periodically review information to determine if it continues to require an OUO or FOUO designation. Based on their comments, we modified the report and our recommendation to focus on the need for periodic oversight of the OUO and FOUO programs.

Also, DOD disagreed with our draft report recommendation that personnel designating a document as FOUO also mark the document with the FOIA exemption used to determine the information should be restricted. We believe that the practice of citing the applicable FOIA exemption(s) will not only increase the likelihood that the information is appropriately marked as FOUO, but will also foster consistent application of the marking throughout DOD. Therefore, we continue to believe our recommendation has merit.

DOE and DOD Lack Clear OUO and FOUO Guidance in Key Aspects

Both DOE and DOD have established offices; designated staff; and promulgated policies, manuals, and guides to provide a framework for the OUO and FOUO programs. However, based on our assessment of the policies governing both DOE's and DOD's programs, their policies to assure that unclassified but sensitive information is appropriately identified and marked lack sufficient clarity in important areas that could allow for inconsistencies and errors. DOE policy clearly identifies the office responsible for the OUO program and establishes a mechanism to mark the FOIA exemption used as the basis for the OUO designation on a document. However, our analysis of DOD's FOUO policies shows that it is unclear which DOD office is responsible for the FOUO program, and

whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document. Also, both DOE's and DOD's policies are unclear regarding at what point a document should be marked as OUO or FOUO, and what would be an inappropriate use of the OUO or FOUO designation. In our view, this lack of clarity exists in both DOE and DOD because the agencies have put greater emphasis on managing classified information, which is more sensitive than OUO or FOUO information.

DOE's OUO program was created in 2003 and DOD's FOUO program has been in existence since 1968. Both programs use the exemptions in FOIA for designating information in a document as OUO or FOUO. Table 1 outlines these exemptions.

Table 1: FOIA Exemptions

Exemption	Examples
1. Classified in accordance with an executive order[a]	Classified national defense or foreign policy information
2. Related solely to internal personnel rules and practices of an agency	Routine internal personnel matters, such as performance standards and leave practices; internal matters the disclosure of which would risk the circumvention of a statute or agency regulation, such as law enforcement manuals
3. Specifically exempted from disclosure by federal statute	Nuclear weapons design (Atomic Energy Act); tax return information (Internal Revenue Code)
4. Privileged or confidential trade secrets, commercial, or financial information	Scientific and manufacturing processes (trade secrets); sales statistics, customer and supplier lists, profit and loss data, and overhead and operating costs (commercial/financial information)
5. Interagency or intra-agency memoranda or letters that are normally privileged in civil litigation	Memoranda and other documents that contain advice, opinions, or recommendations on decisions and policies (deliberative process); documents prepared by an attorney in contemplation of litigation (attorney work-product); confidential communications between an attorney and a client (attorney-client)
6. Personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy	Personal details about a federal employee, such as date of birth, marital status, and medical condition
7. Records compiled for law enforcement purposes where release either would or could harm those law enforcement efforts in one or more ways listed in the statute	Witness statements; information obtained in confidence in the course of an investigation; identity of a confidential source
8. Certain records and reports related to the regulation or supervision of financial institutions	Bank examination reports and related documents
9. Geographical and geophysical information and data, including maps, concerning wells	Well information of a technical or scientific nature, such as number, locations, and depths of proposed uranium exploration drill-holes

Sources: FOIA and GAO analysis.

[a]As noted earlier in this report, classified information is not included in DOE's and DOD's OUO and FOUO programs.

The Federal Managers Financial Improvement Act of 1982 states that agencies must establish internal administrative controls in accordance with the standards prescribed by the Comptroller General.[5] The Comptroller General published such standards in *Standards for Internal Control in the Federal Government*, which sets out management control standards for all aspects of an agency's operation. These standards are intended to provide reasonable assurance of meeting agency objectives, and should be recognized as an integral part of each system that management uses to regulate and guide its operations. One of the standards of internal control—internal control activities—states that appropriate policies, procedures, techniques, and mechanisms should exist with respect to each of the agency's activities and are an integral part of an agency's planning, implementing, and reviewing.

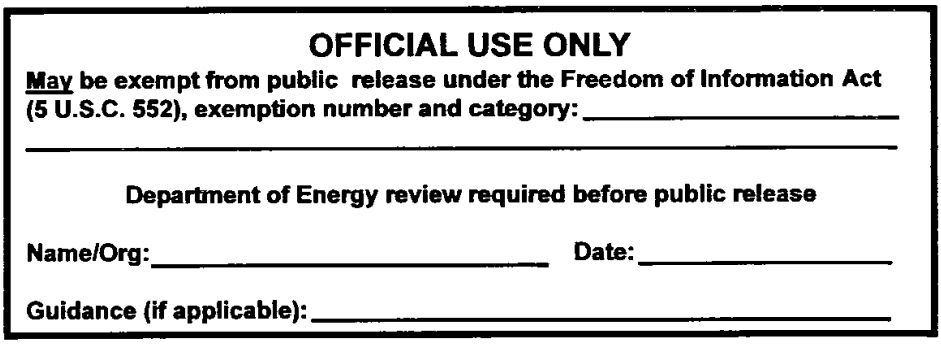
DOE's Office of Security issued an order, a manual, and a guide in April 2003 to detail the requirements and responsibilities for DOE's OUO program and to provide instructions for identifying, marking, and protecting OUO information.[6] According to DOE officials, the agency issued the order, manual, and guide to provide guidance on how and when to identify information as OUO and eliminate various additional markings, such as Patent Caution or Business Sensitive, for which there was no law, regulation, or DOE directive to inform staff how such documents should be protected. The overall goal of the order was to establish a policy consistent with criteria established in FOIA. DOE's order established the OUO program and laid out, in general terms, how sensitive information should be identified and marked, and who is responsible for doing so. The guide and the manual supplement the order. The guide provides more detailed information on the eight applicable FOIA exemptions to help staff decide whether exemption(s) may apply, which exemption(s) may apply, or both. The manual provides specific instructions for managing OUO information, such as mandatory procedures and processes for properly identifying and marking this information. For example, the employee marking a document is required to place on the front page of the document an OUO stamp that has a space for the employee to identify

[5]Pub. L. No. 97-255 (Sept. 8, 1982).

[6]DOE Order 471.3, *Identifying and Protecting Official Use Only Information*, contains responsibilities and requirements; DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, provides instructions for implementing requirements; and DOE Guide 471.3-1, *Guide to Identifying Official Use Only Information*, provides information to assist staff in deciding whether information could be OUO.

which FOIA exemption is believed to apply; the employee's name and organization; the date; and, if applicable, any guidance the employee may have used in making this determination.[7] According to one senior DOE official, requiring the employee to cite a reason why a document is designated as OUO is one of the purposes of the stamp, and one means by which DOE's Office of Classification encourages practices consistent with the order, guide, and manual throughout DOE. Figure 1 shows the DOE OUO stamp.

Figure 1: DOE's OUO Stamp



Source: DOE.

The current DOD regulations are unclear regarding which DOD office controls the FOUO program. Although responsibility for the FOUO program was shifted from the Director for Administration and Management to the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (now the Under Secretary of Defense, Intelligence) in October 1998, this shift is not reflected in current regulations. Guidance for DOD's FOUO program continues to be included in regulations issued by both offices. As a result, there is currently a lack of clarity regarding which DOD office has primary responsibility for the FOUO program. According to a DOD official, this lack of clarity causes personnel who have FOUO questions to contact the wrong office. The direction provided in *Standards for Internal Control in the Federal Government* states that an agency's organizational structure

[7]DOE classification guides used for managing classified information sometimes include specific guidance on what information should be protected and managed as OUO. When such specific guidance is available to the employee, he or she is required to mark the document accordingly.

should clearly define key areas of authority and responsibility. A DOD official said that they began coordination of a revised Information Security regulation covering the FOUO program at the end of January 2006. The new regulation will reflect the change in responsibilities and place greater emphasis on the management of the FOUO program.

DOD currently has two regulations, issued by each of the offices described above, containing similar guidance that addresses how unclassified but sensitive information should be identified, marked, handled, and stored.[8] Once information in a document has been identified as FOUO, it is to be marked For Official Use Only. However, unlike DOE, DOD has no departmentwide requirement to indicate which FOIA exemption may apply to the information, except when it has been determined to be releasable to a federal governmental entity outside of DOD. We found, however, that one of the Army's subordinate commands does train its personnel to put an exemption on any documents that are marked as FOUO, but does not have this step as a requirement in any policy. In our view, if DOD were to require employees to take the extra step of marking the exemption that may be the reason for the FOUO designation at the time of document creation, it would help assure that the employee marking the document has at least considered the exemptions and made a thoughtful determination that the information fits within the framework of the FOUO designation. Including the FOIA exemption on the document at the time it is marked would also facilitate better agency oversight of the FOUO program since it would provide any reviewer/inspector with an indication of the basis for the marking.

Both DOE's and DOD's policies are unclear at what point to actually affix the OUO or FOUO designation to a document. If a document is not marked at creation, but might contain information that is OUO or FOUO and should be handled as such, it creates a risk that the document could be mishandled. DOE policy is vague about the appropriate time to apply a marking. DOE officials in the Office of Classification stated that their policy does not provide specific guidance about at what point to mark a document because such decisions are highly situational. Instead, according to these officials, the DOE policy relies on the "good judgment" of DOE personnel in deciding the appropriate time to mark a document.

[8]DOD 5400.7-R, *DOD Freedom of Information Act Program* (Sept. 4, 1998); DOD 5200.1-R, *Information Security Program* (Jan. 14, 1997); and interim changes to DOD 5200.1-R, *Information Security Regulation*, *Appendix 3: Controlled Unclassified Information* (April 2004).

Similarly, DOD's current Information Security regulation addressing the FOUO program does not identify when a document should be marked. In contrast, DOD's September 1998 FOIA regulation, in a chapter on FOUO, states that "the marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is requested under the FOIA." In our view, a policy can provide flexibility to address highly situational circumstances and also provide specific guidance and examples of how to properly exercise this flexibility.

In addition, we found both DOE's and DOD's OUO and FOUO programs lack clear language identifying examples of inappropriate use of OUO or FOUO markings. According to *Standards for Internal Control in the Federal Government*, agencies should have sufficient internal controls in place to mitigate risk and assure that employees are aware of what behavior is acceptable and what is unacceptable. Without explicit language identifying inappropriate use of OUO or FOUO markings, DOE and DOD cannot be confident that their personnel will not use these markings to conceal mismanagement, inefficiencies, or administrative errors or to prevent embarrassment to themselves or their agency.[9]

Neither DOE nor DOD Requires Training or Conducts Oversight

Standards for Internal Control in the Federal Government discusses the need for both training and continuous program monitoring as necessary components of a good internal control program. However, while both DOE and DOD offer training to staff on managing OUO and FOUO information, neither agency requires any training of its employees before they are allowed to identify and mark information as OUO or FOUO, although some staff will eventually take OUO or FOUO training as part of other mandatory training. In addition, neither agency has implemented an oversight program to determine the extent to which employees are complying with established policies and procedures. DOE and DOD officials told us that limited resources, and in the case of DOE, the newness of the program, have contributed to the lack of training requirements and oversight.

OUO and FOUO Training Is Generally Not Required

While many DOE units offer training on DOE's OUO policy, DOE does not have a departmentwide policy that requires OUO training before an

[9]Similar language is included in DOD's policies regarding protection of national security information (DOD 5200.1-R, *Information Security Program*, (Jan. 14, 1997), sec. C2.4.3.1). DOE's policy for protecting national security information (DOE M 475.1-1A) makes reference to Executive Order 12958, as amended, which also has similar language.

employee is allowed to designate a document as OUO. As a result, some DOE employees may be identifying and marking documents for restriction from dissemination to the public or persons who do not need to know the information to perform their jobs and yet may not be fully informed as to when it is appropriate to do so. At DOE, the level of training that employees receive is not systematic and varies considerably by unit, with some requiring OUO training at some point as a component of other periodic employee training, and others having no requirements at all. For example, most of DOE's approximately 10,000 contractor employees at the Sandia National Laboratories in Albuquerque, New Mexico, are required to complete OUO training as part of their annual security refresher training. In contrast, according to the senior classification official at Oak Ridge, very few staff received OUO training at DOE's Oak Ridge Office in Oak Ridge, Tennessee, although staff were sent general information about the OUO program when it was launched in 2003 and again in 2005. Instead, this official provides OUO guidance and other reference and training materials to senior managers with the expectation that they will inform their staff on the proper use of OUO.

DOD similarly has no departmentwide training requirements before staff are authorized to identify, mark, and protect information as FOUO. The department relies on the individual services and components within DOD to determine the extent of training employees receive. When training is provided, it is usually included as part of a unit's overall security training, which is required for many but not all employees. There is no requirement to track which employees received FOUO training, nor is there a requirement for periodic refresher training. Some DOD components, however, do provide FOUO training for employees as part of their security awareness training.

Oversight of OUO and FOUO Programs Is Lacking

Neither DOE nor DOD knows the level of compliance with OUO and FOUO program policies and procedures because neither agency conducts any oversight to determine whether the OUO and FOUO programs are being managed well. According to a senior manager in DOE's Office of Classification, the agency does not review OUO documents to assess whether they are properly identified and marked. This condition appears to contradict the DOE policy requiring the agency's senior officials to assure that the OUO programs, policies, and procedures are effectively implemented. Similarly, DOD does not routinely review FOUO information to assure that it is properly managed.

Without oversight, neither DOE nor DOD can assure that staff are complying with agency policies. We are aware of at least one recent case in which DOE's OUO policies were not followed. In 2005, there were several stories in the news about revised estimates of the cost and length of the cleanup of high-level radioactive waste at DOE's Hanford Site in southeastern Washington. This information was controversial because there is a history of delays and cost overruns associated with this multibillion dollar project, and DOE was restricting a key document containing recently revised cost and time estimates from being released to the public. This document, which was produced by the U.S. Army Corps of Engineers for DOE, was marked Business Sensitive by DOE. However, according to a senior official in the DOE Office of Classification, Business Sensitive is not a recognized marking in DOE. Therefore, there is no DOE policy or guidance on how to handle or protect documents marked with this designation. This official said that if information in this document needed to be restricted from release to the public, then the document should have been stamped OUO and the appropriate FOIA exemption should have been marked on the document.

Conclusions

The lack of clear policies, effective training, and oversight in DOE's and DOD's OUO and FOUO programs could result in both over- and underprotection of unclassified yet sensitive government documents that may need to be limited from disclosure to the public or persons who do not need to know such information to perform their jobs to prevent potential harm to governmental, commercial, or private interests. Having clear policies and procedures in place, as discussed in *Standards for Internal Control in the Federal Government*, can mitigate the risk that programs could be mismanaged and can help DOE and DOD management assure that OUO or FOUO information is appropriately marked and handled. DOE and DOD have no systemic procedures in place to assure that staff are adequately trained before designating documents OUO or FOUO, nor do they have any means of knowing the extent to which established policies and procedures for making these designations are being complied with. These issues are important because they affect DOE's and DOD's ability to assure that the OUO and FOUO programs are identifying, marking, and safeguarding documents that truly need to be protected in order to prevent potential damage to governmental, commercial, or private interests.

Recommendations for Executive Action

To assure that the guidance governing the FOUO program reflects the necessary internal controls for good program management, we recommend that the Secretary of Defense take the following two actions:

- revise the regulations that currently provide guidance on the FOUO program to conform to the 1998 policy memo designating which office has responsibility for the FOUO program and
- revise any regulation governing the FOUO program to require that personnel designating a document as FOUO also mark the document with the FOIA exemption used to determine the information should be restricted.

We also recommend that the Secretaries of Energy and Defense take the following two actions to clarify all guidance regarding the OUO and FOUO designations:

- identify at what point the document should be marked as OUO or FOUO and
- define what would be an inappropriate use of the designations OUO or FOUO.

To assure that OUO and FOUO designations are correctly and consistently applied, we recommend that the Secretaries of Energy and Defense take the following two actions:

- assure that all employees authorized to make OUO and FOUO designations receive an appropriate level of training before they can mark documents and
- develop a system to conduct periodic oversight of OUO and FOUO designations to assure that information is being properly marked and handled.

Agency Comments and Our Evaluation

In commenting on a draft of this report, both DOE and DOD agreed with the findings of the report and with most of the report's recommendations. DOE agreed with our recommendations to clarify its guidance to identify at what point a document should be marked OUO and define what would be an inappropriate use of OUO. They also agreed with our recommendation that all employees authorized to make OUO designations receive training before they can mark documents. DOD concurred with our recommendations to revise the regulations designating which office has responsibility for the FOUO program, to clarify guidance regarding at what point to mark a document as FOUO and to define inappropriate

usage of the FOUO designation, and to assure that all employees authorized to make FOUO designations receive appropriate training.

Both DOE and DOD partially concurred with our recommendation to develop a system to conduct periodic oversight of OUO or FOUO designations. They agreed with developing a system for periodic oversight of OUO or FOUO designations, but disagreed with the recommendation in our draft report to conduct period reviews of OUO or FOUO information to determine if the information continues to require that designation. DOE stated that much of the information designated as OUO is permanent by nature—such as information related to privacy and proprietary interests—and a systematic review would "primarily serve to correct a small error rate that would be better addressed by additional training and oversight." In its comments, DOD stated that such a review would not be an efficient use of limited resources because "all DOD information, whether marked as FOUO or not, is specifically reviewed for release when disclosure to the public is desired by the Department or requested by others. Any erroneous or improper designation as FOUO is identified and corrected in this review process and the information released as appropriate. Thus, information is not withheld from the public based solely on the initial markings applied by the originator." Based on DOE's and DOD's comments, we believe the agencies have agreed to address the principal concern that led to our original recommendation. We therefore have modified the report and our recommendation to focus on the need for periodic oversight of the OUO and FOUO programs by deleting the portion of the recommendation calling for a periodic review of the information to determine if it continues to require an OUO or FOUO designation.

DOD did not concur with our recommendation to require that personnel designating a document as FOUO also mark the document with the applicable FOIA exemption(s). DOD stated that "if the individual erroneously applies an incorrect/inappropriate FOIA exemption to a document, then it is possible that other documents that are derivatively created from this document would also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. Additionally, when the document is reviewed for release to the public, the annotated FOIA exemption may cause the reviewer to believe that the document is automatically exempt from release and not perform a proper review." However, we believe that the practice of citing the applicable FOIA exemption(s) will not only increase the likelihood that the information is appropriately marked as FOUO, but will also foster consistent application of the marking throughout DOD. Using a stamp similar to the one employed by DOE (see fig. 1), which clearly states that

the marked information may be exempt from public release under a specific FOIA exemption, should facilitate the practice. Furthermore, as DOD stated above, "all DOD information, whether marked as FOUO or not, is specifically reviewed for release when disclosure to the public is desired by the Department or requested by others. Any erroneous or improper designation as FOUO is identified and corrected in this review process and the information released as appropriate. Thus, information is not withheld from the public based solely on the initial markings applied by the originator." Therefore, if DOD, under the FOIA process, properly reviews all documents before they are released and corrects any erroneous or improper designation, then prior markings should not affect the decision to release a document, particularly if such markings are identified as provisional. Therefore, we continue to believe our recommendation has merit.

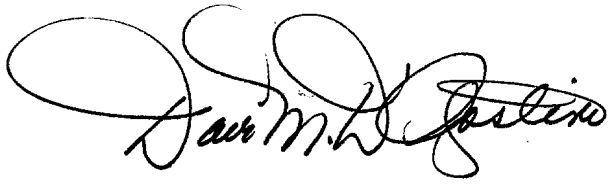
Comments from DOE's Director, Office of Security and Safety Performance Assurance and DOD's Deputy Under Secretary of Defense (Counterintelligence and Security) are reprinted in appendix I and appendix II, respectively. DOE and DOD also provided technical comments, which we included in the report as appropriate.

As agreed with your offices unless you publicly release the contents of this report earlier, we plan no further distribution until 30 days from its date. We will then send copies of this report to the Secretary of Energy; the Secretary of Defense; the Director, Office of Management and Budget; and interested congressional committees. 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.

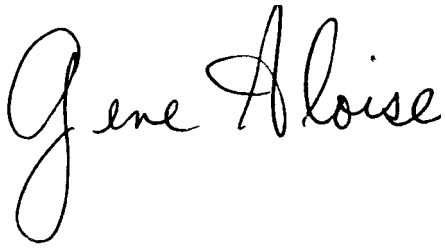
If you or your staff have any questions concerning this report, please contact either of us. Davi M. D'Agostino can be reached at (202) 512-5431 or dagostinod@gao.gov, and Gene Aloise can be reached at (202) 512-3841 or aloisee@gao.gov. Contact points for our Offices of Congressional

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



Gene Aloise
Director, Natural Resources and Environment

Appendix I: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

February 7, 2006

Mr. Gene Aloise
Director
Natural Resources and Environment Team
United States Government Accountability Office
Washington, D.C. 20548

Dear Mr. Aloise:

The Department of Energy (DOE) has completed its review of the Government Accountability Office (GAO) draft report GAO-06-369, MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved. We understand the report is one of three that resulted from a request by The Honorable Christopher Shays to review information classification management at the Department of Energy and the Department of Defense (DOD). This review was specifically to (1) identify and assess the policies, procedures, and criteria the DOE and the DOD employ to manage Official Use Only (OUO) and For Official Use Only (FOUO) information and (2) determine the extent to which DOE's and DOD's training and oversight programs assure that information is identified, marked, and protected according to established criteria.

The DOE agrees that the findings are accurate and concurs with all but one recommendation as discussed below. Since the 2003 publication of DOE Order 471.3, *Identifying and Protecting Official Use Only Information,* DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE Guide 471.3-1, *Guide to Identifying Official Use Only Information,* DOE efforts have focused on education and assistance. The DOE has assisted its organizations by providing training and reviewing OUO training materials produced by program offices as requested, and by responding to questions. In addition, Headquarters personnel met with field personnel regarding OUO training and program implementation during classification oversight reviews. Despite these efforts, we agree with the GAO that the DOE OUO program is implemented unevenly. Therefore, we agree that OUO training should be required for all employees and that OUO should be included as an element of oversight reviews. The DOE plans to revise OUO directives to add training and oversight requirements. These actions should ensure OUO information is identified accurately and consistently throughout the DOE. In addition, the directives will be revised, as recommended, to include information on the inappropriate use of OUO and clarify the point at which a document containing OUO information should be marked.

However, we disagree with the GAO recommendation for periodic review of OUO information. Most OUO documents are in collections that do not have permanent historical value, for which there is no public interest, and that are destroyed without ever having been requested. Documents are currently reviewed as requested and when they are scheduled

Printed with soy ink on recycled paper

for release. The DOE believes this approach represents the most efficient method of providing information to the public and best matches the public interest to taxpayer cost.

Periodic review is also unnecessary because it would likely result in few changes to OUO determinations. Unlike classified information, which may be declassified or subject to declassification dates or events, the Freedom of Information Act (FOIA) basis for OUO information is stable, and much of the information is permanent by nature. OUO is consistent with FOIA exemptions, which, except for minor additions, have been stable since the law was enacted in 1966. Certain exemptions, such as privacy and proprietary exemptions, are permanent in nature. Systematic review would primarily serve to correct a small error rate that would be better addressed by additional training and oversight.

Although systematic review is inadvisable, we agree that some quality control is prudent. We, therefore, plan to include the review of OUO documents in oversight reviews and to revise DOE directives to require document reviews for OUO in field-conducted oversight reviews and self-assessments.

We also plan to take a pro-active approach to lessen the likelihood of incorrect OUO determinations. Revising DOE directives for clarity and requiring additional training and oversight should improve the implementation of the OUO program and decrease the likelihood of documents being incorrectly marked or not marked as OUO. Our planned actions, as detailed in the appendix, should provide sufficient education and quality control to ensure that the DOE's OUO program is consistent and accurate. We feel these actions represent a cost effective solution to improving the DOE's OUO program.

Sincerely,

Glenn S. Podonsky
Director
Office of Security and Safety
Performance Assurance

Enclosures

Appendix

DOE Response to GAO Draft Report
MANAGING SENSITIVE INFORMATION:
Departments of Energy and Defense Policies and Oversight Could Be Improved
(GAO-06-369)

In summary, the DOE finds the draft report to be a fair evaluation of its Official Use Only (OUO) program. The DOE plans the following specific actions related to recommendations in the draft report:

Recommendation 1. We recommend that the Secretaries of Energy and Defense clarify all guidance regarding the OUO and FOUO designations:

- To identify when the document should be marked as "OUO" or "FOUO" and
- To define what would be an inappropriate use of the designations "OUO" or "FOUO."

DOE Response. The DOE plans to revise DOE Order 471.3, *Identifying and Protecting Official Use Only Information,* and DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, to clarify the point at which OUO markings should be applied to a document.

The DOE also plans to revise the above directives to include a discussion of the inappropriate use of OUO.

Recommendation 2. Assure that all employees authorized to make OUO and FOUO designations receive an appropriate level of training before they can mark documents.

DOE Response. The DOE plans to revise DOE directives to require initial and refresher OUO training and identify the persons responsible for ensuring training is implemented and conducted.

Recommendation 3. Develop a system to conduct periodic oversight of OUO and FOUO designations to assure that information is being properly marked and handled and that a periodic review of the information is done to determine if the information continues to be OUO.

DOE Response. The DOE plans to implement an OUO oversight program to include an evaluation of the identifying, marking, and protection of OUO information using lines of inquiry based on DOE directives and guidance. The program will be developed and incorporated into the Classification and Information Control Oversight Program. Oversight reviews will include the review of documents marked OUO and unmarked documents to ensure OUO determinations are appropriate and consistent, and the correct exemptions are cited. In addition, the DOE plans to revise the OUO directives to add the evaluation of the

identification, marking, and protection of OUO as a requirement for field oversight reviews and self-assessments.

The DOE does not plan to develop a program for systematic review of OUO documents. The current approach of reviewing documents as requested and when they are scheduled for release represents the most efficient method of providing information to the public and best matches the public interest to taxpayer cost. The DOE feels increased training and oversight will produce a more consistent and accurate OUO program sufficiently responsive to public interest.

Appendix II: Comments from the Department of Defense

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

INTELLIGENCE

FEB 0 7 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:

This is the Department of Defense (DoD) response to the GAO draft report, "MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved," dated January 23, 2006, (GAO Code 350774/GAO-06-369).

The DoD agrees that policy regarding use of the "For Official Use Only" (FOUO) designation could be clarified and changes to do so are included in the revision of DoD Regulation 5200.1, "DoD Information Security Program," which is currently underway. Additional guidance will be incorporated to include changes suggested by the GAO. However, the DoD disagrees with the GAO's recommendations that the designator annotate the applicable FOIA exemption and that documents so marked be periodically reviewed to determine if the information continues to require the FOUO designation.

Detailed comments on each of the specific recommendations in the draft report are attached.

Sincerely,

ACTING

Robert W. Rogalski
Deputy Under Secretary of Defense
(Counterintelligence and Security)

GAO DRAFT REPORT - DATED JANUARY 23, 2006
GAO CODE 350774/GAO-06-369

"MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved"

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense revise the regulations that currently provide guidance on the FOUO program to conform to the 1998 policy memo designating which office has responsibility for the FOUO program. (p. 13/GAO Draft Report)

DOD RESPONSE: Concur. This requirement will be addressed as part of the on-going revisions of DoD Regulation 5200.1, "DoD Information Security Program," and DoD Regulation 5400.7, "Freedom of Information Act Program."

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense revise any regulation governing the FOUO program to require that personnel designating a document as "FOUO" also mark the document with the applicable FOIA exemption used to determine the information should be restricted. (p. 13/GAO Draft Report)

DOD RESPONSE: Non-concur. The Department does not concur with the GAO recommendation that the personnel designating an original document as "FOUO" also annotate the marking with the appropriate FOIA exemption. If the individual erroneously applies an incorrect/inappropriate FOIA exemption to a document, then it is possible that other documents that are derivatively created from this document would also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. Additionally, when the document is reviewed for release to the public, the annotated FOIA exemption may cause the reviewer to believe that the document is automatically exempt from release and not perform a proper review.

RECOMMENDATION 3: The GAO recommended that the Secretaries of Energy and Defense clarify all guidance regarding the OUO and FOUO designations:

- to identify when the document should be marked as "OUO" or "FOUO"; and ,
- to define what would be an inappropriate use of the designations "OUO" or "FOUO."

(p. 14/GAO Draft Report)

DOD RESPONSE: Concur. These requirements will be added to the guidance regarding FOUO information in the revision of DoD 5200.1-R that is underway.

RECOMMENDATION 4: The GAO recommended that the Secretaries of Energy and Defense assure that all employees authorized to make OUO and FOUO designations receive an appropriate level of training before they can mark documents. (p. 14/GAO Draft Report)

DOD RESPONSE: Concur. The revision to DoD 5200.1-R will specify that all personnel shall receive training that provides a basic understanding of the nature of controlled unclassified information and to ensure proper protection of such information in their possession.

RECOMMENDATION 5: The GAO recommended that the Secretaries of Energy and Defense develop a system to conduct periodic oversight of OUO and FOUO designations to assure that information is being properly marked and handled and that a periodic review of the information is done to determine if the information continues to require an OUO/FOUO designation. (p. 14/GAO Draft Report)

DOD RESPONSE: Partially Concur. The Department concurs with the recommendation to develop a system to conduct periodic oversight of FOUO designations and will include that requirement as part of the Information Security Program oversight process. The Department non-concurs with the requirement to conduct periodic reviews of FOUO information to determine if the information continues to require that designation. Except to the extent that FOUO information is included in a classification guide and is reviewed as part of a classified program requirement, such a review is not an efficient use of limited Departmental resources. Designation as FOUO does not limit information dissemination to the public but rather serves to inform DoD personnel that the information may qualify for withholding and that extra caution should be taken in handling the information. All DoD information, whether marked as FOUO or not, is specifically reviewed for release when disclosure to the public is desired by the Department or requested by others. Any erroneous or improper designation as FOUO is identified and corrected in this review process and the information released as appropriate. Thus, information is not withheld from the public based solely on the initial markings applied by the originator. Additionally, it is not clear that a sufficient number of FOUO designations would change with the passage of time to justify the resource expenditure as the basis for many of the exemptions is not time-related (e.g., proprietary, Privacy, statutory).

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Davi M. D'Agostino (202) 512-5431 or dagostinod@gao.gov
Gene Aloise (202) 512-3841 or aloisee@gao.gov

Acknowledgments

In addition to the contacts named above, Ann Borseth and Ned Woodward, Assistant Directors; Nancy Crothers; Doreen Feldman; Mattias Fenton; Adam Hatton; David Keefer; William Lanouette; Gregory Marchand; David Mayfield; James Reid; Marc Schwartz; Kevin Tarmann; 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

PRINTED ON RECYCLED PAPER