United States Government Accountability Office

GAO

Testimony

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

For Release on Delivery
Expected at 2:00 p.m. EST
Tuesday, March 14, 2006

MANAGING SENSITIVE INFORMATION

DOE and DOD Could Improve Their Policies and Oversight

Statement of Davi M. D'Agostino, Director
Defense Capabilities and Management, and
Gene Aloise, Director
Natural Resources and Environment

March 14, 2006

MANAGING SENSITIVE INFORMATION

DOE and DOD Could Improve Their Policies and Oversight

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-531T, a testimony 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

In its report issued earlier this month, 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 mark it with the applicable FOIA exemption.

www.gao.gov/cgi-bin/getrpt?GAO-06-531T.

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

As GAO reported earlier this month, 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. While DOE and DOD have policies in place to manage their OUO or FOUO programs, our analysis of these policies showed a lack of clarity in key areas that could allow inconsistencies and errors to occur. 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 conceal 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.

In addition, 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. 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.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our work on how the Departments of Energy (DOE) and Defense (DOD) use the designations Official Use Only (OUO) and For Official Use Only (FOUO), respectively, to manage information that is unclassified but sensitive. My testimony today is based on our report issued earlier this month entitled *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved* (GAO-06-369). This report (1) identified and assessed the policies, procedures, and criteria that DOE and DOD employ to manage OUO and FOUO information; and (2) determined the extent to which DOE's and DOD's training and oversight programs assure that information is identified and marked according to established criteria.

In summary, 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.[1] (See the appendix for a list and description of the exemptions of FOIA.) Both agencies have policies in place to implement their programs. However, our analysis of these policies showed a lack of clarity in key areas that could allow inconsistencies and errors to occur. Specifically:

- 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.
- 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 conceal agency mismanagement.

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

In addition, 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. This lack of training requirements and oversight 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 recommended that both agencies clarify their policies and guidance to identify at what point a document should be marked as OUO or FOUO and to define inappropriate uses of these designations. We also recommended that DOD clarify its policies as to which office is responsible for the FOUO program and that it require personnel designating a document as FOUO also to note the FOIA exemption they used to determine that the information should be restricted. With regard to training and management oversight, we recommended that both DOE and DOD require personnel to be trained before they can designate information as OUO or FOUO, and that they develop a system to conduct periodic oversight of OUO or FOUO designations to assure that their policies are being followed.

In commenting on our draft report, DOE and DOD agreed with most of our recommendations, but DOD disagreed that personnel designating a document as FOUO should also mark the document with the FOIA exemption used to determine that the information should be restricted. DOD expressed concern that an individual may apply an incorrect or inappropriate FOIA exemption and thus cause other documents that are created from the original to also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. However, we believe that citing the applicable FOIA exemptions when marking a document will cause the employee to consider the exemptions and make a thoughtful determination that the information fits within the framework of the FOUO designation. Also, when the public requests documents, before DOD releases or denies release of the documents, FOIA experts review them, at which time an incorrect initial designation should be corrected. Our recommendation was intended to better assure appropriate consideration of the FOIA exemptions at the beginning of the process and we continue to believe that this recommendation has merit.

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

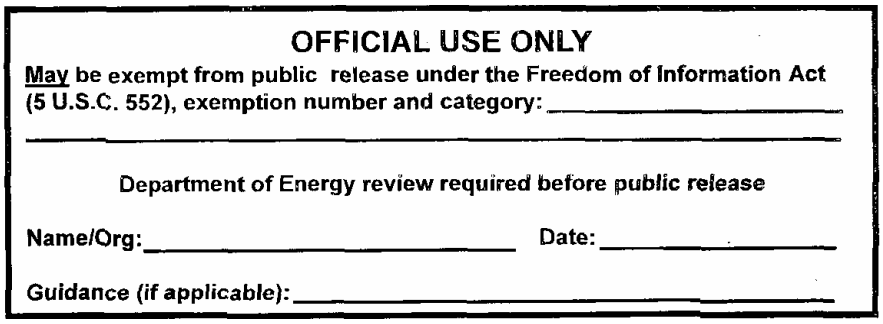
Both DOE and DOD have established offices, designated staff, and promulgated policies to provide a framework for the OUO and FOUO programs. However, their policies lack sufficient clarity in important areas, which could result in inconsistencies and errors. DOE policy clearly identifies the office responsible 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 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.[2] 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 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 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

[2]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.

determination.[3] 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.

With regard to DOD, its regulations are unclear regarding which DOD office controls the FOUO program. Although responsibility for the FOUO program 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, which DOD office has primary responsibility for the FOUO program is unclear. According to a DOD official, on occasion this lack of clarity causes personnel who have FOUO questions to contact the wrong office. A DOD official said that the department 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.

[3]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.

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.[4] Once information in a document has been identified as for official use only, it is to be marked FOUO. 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 had at least considered the exemptions and made a thoughtful determination that the information fit 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.

In addition, both DOE's and DOD's policies are unclear as to the point at which the OUO or FOUO designation should actually be affixed to a document. If a document might contain information that is OUO or FOUO but it is not so marked when it is first created, the risk that the document could be mishandled increases. 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. Similarly, DOD's current Information Security regulation addressing the FOUO program does not identify at what point 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

[4]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* (Apr. 16, 2004).

requested under the FOIA."[5] 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 that both DOE's and DOD's OUO and FOUO programs lack clear language identifying examples of inappropriate usage of OUO or FOUO markings. Without such language, 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.[6]

Neither DOE nor DOD Requires Training or Conducts Oversight

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.

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 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.

[5]DOD 5400.7-R, C4.1.4, p.43.

[6]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, *Classified National Security Information*, as amended, which also has similar language.

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 field activities within DOD to determine the extent of training that 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 conduct oversight of its FOUO program 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, several stories appeared 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 this multibillion-dollar project has a history of delays and cost overruns, 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.

In closing, 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. Having clear policies and procedures in place can mitigate the risk of program mismanagement 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.

Mr. Chairman, this concludes GAO's prepared statement. We would be happy to respond to any questions that you or Members of the Subcommittee may have.

GAO Contacts and Staff Acknowledgments

For further information on this testimony, please contact either Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov, or Gene Aloise 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 statement. Individuals making key contributions to this testimony included Ann Borseth, David Keefer, Kevin Tarmann, and Ned Woodward.

Appendix: 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.

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