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

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

GAO-06-785

June 2006

MANAGING SENSITIVE INFORMATION

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

GAO Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

What GAO Recommends

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

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

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

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

What GAO Found

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

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

Contents

Abbreviations

AEA	Atomic Energy Act
C/FGI-MOD	Confidential Foreign Government Information–Modified Handling Authorized
CRD	Confidential Restricted Data
DOD	Department of Defense
DOE	Department of Energy
FRD	Formerly Restricted Data
NNPI	Naval Nuclear Prolusion Information
NNSA	National Nuclear Security Administration
NSI	National Security Information
RD	Restricted Data
SRD	Secret Restricted Data
TSRD	Top Secret Restricted Data
UCNI	Unclassified Controlled Nuclear Information

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
U.S. House of Representatives

Dear Mr. Chairman:

In recent years, the Congress has become increasingly concerned that federal agencies are misclassifying information.[1] Classified information is material containing national defense or foreign policy information determined by the U.S. government to require protection for reasons of national security. Access to classified information generally requires a security clearance. The number of classified documents is unknown because there is no requirement to account for most of them; however, some estimates put their number in the hundreds of millions. In just the past 5 fiscal years for which data are available (2000 to 2004), federal agencies created more than 110 million new classified documents. From 2000 through 2005, the Department of Energy (DOE) classified about 234,000 documents, including a record 62,281 documents in 2004 and about 58,000 documents in 2005. DOE is responsible for most of the U.S. government's information about nuclear weapons and technology. Managing classified information is one of the most important responsibilities that an agency has because underclassifying, wrongly declassifying, and overclassifying sensitive information can all endanger national security. While it is obvious that underclassifying or wrongly

[1]We issued a report on the management of sensitive but unclassified information at the Departments of Energy and Defense. See GAO, *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved*, GAO-06-369 (Washington, D.C.: Mar. 7, 2006). We also issued a report on the status of the federal government's policies and processes to share classified and sensitive but unclassified terrorism-related information. See GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006). We are also issuing a report on the Department of Defense's management of classified information. See GAO, *Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors*, GAO-06-706 (Washington, D.C.: June 30, 2006).

declassifying a document can lead to the improper release of vital information, overclassifying can also have damaging consequences. For example, the *9/11 Commission Report* concluded that policies designed to protect government information have led to overclassification, which has inhibited information sharing among federal agencies.[2]

According to officials at the National Archives' Information Security Oversight Office, which is responsible for setting federal government policy for managing classified information, an effective classification management program is based on a strong system of internal controls, including training, guidance, and oversight. From the 1950s until 2005, DOE's Office of Classification and its predecessor offices provided expertise as well as systematic training, extensive guidance, and effective oversight. As part of DOE's Office of Security and Safety Performance Assurance, the Office of Classification provided training at DOE headquarters, field sites, and program offices in how to identify, mark, and protect classified information and documents. This office also developed an extensive collection of classification guides, or manuals, specifying precisely which information must be classified. However, in October 2005, DOE shifted responsibility for oversight from the Office of Classification to the Office of Security Evaluations—another office within the Office of Security and Safety Performance Assurance—which is primarily responsible for the oversight of physical security at DOE sites containing nuclear materials.

This report assesses the extent to which (1) DOE's training, guidance, and oversight ensure that information is classified and declassified according to established criteria and (2) DOE has found documents to be misclassified.

To assess the extent to which DOE's training and oversight ensure information is classified and declassified appropriately, we analyzed the policies and procedures used at various DOE sites and national laboratories to determine if authorized classifiers and declassifiers had up-to-date training and guidance. Where applicable, we assessed the reliability of the data and found them sufficiently reliable for the purposes of this report. In addition, to better understand DOE's training program, its process for certifying classifiers and declassifiers, as well as the

[2]See *9/11 Commission Report*, *National Commission on Terrorist Attacks Upon the United States*, July 2004, available at http://www.9-11commission.gov/.

department's classification and declassification procedures, we completed DOE's core training for classifying and declassifying documents. We also met with officials responsible for managing classification activities in DOE headquarters units and managers at six DOE sites: two in Albuquerque and one in Los Alamos, New Mexico; one in Aiken, South Carolina; and two in Oak Ridge, Tennessee. To assess the extent to which DOE has found documents to be misclassified, we analyzed the 34 classification inspections by DOE's Office of Classification and its predecessor offices, between 2000 and 2005.[3] We did not independently review classified documents because the technical expertise required to make valid judgments about the classification of nuclear weapons and technology was not available to us outside DOE. We also met with officials from the Information Security Oversight Office of the National Archives and Records Administration to obtain their views on the elements of a successful classification program as well as their evaluations of how DOE manages classified information. We conducted our work from April 2005 to May 2006 in accordance with generally accepted government auditing standards.

Results in Brief

In recent years, DOE's Office of Classification's systematic training, comprehensive guidance, and rigorous oversight programs have, to a great extent, helped to ensure that information is classified and declassified according to established criteria. However, an October 2005 shift in responsibility for classification oversight to the Office of Security Evaluations has created uncertainty about whether a high level of performance in oversight will be sustained. Specifically, prior to this shift, the Office of Classification had performed 34 inspections of classification programs at DOE sites since 2000—including an average of about 10 each year for 2004 and 2005. These inspections reviewed whether DOE sites complied with agency classification policies and procedures. For example, each site we visited had systems in place to ensure that staff authorized to classify documents had completed required training as well as complete and up-to-date classification guides. Our findings are consistent with those of the National Archives' Information Security Oversight Office, which evaluated DOE's management of classified information in September 2005 and found it to be among the best in the federal government. As part of its

[3]We included National Nuclear Security Administration (NNSA) sites in our review because much of DOE's classification activity occurs in NNSA. NNSA is a separately organized agency within DOE responsible for the management and security of the nation's nuclear weapons, nonproliferation, and naval reactor programs.

required annual self-assessment, a site's classification officer documents the steps taken to ensure that all staff authorized to classify or declassify documents are up-to-date on their training and classification guidance. In addition, most sites we visited had gone through an Office of Classification oversight inspection within the previous 2 years. After the October 2005 shift, however, the pace of this oversight was interrupted as classification oversight activities ceased until February 2006. So far in 2006, one classification oversight report has been completed for two offices at DOE's Pantex Site in Texas, and work on a second report is under way at four offices at the Savannah River Site in South Carolina. In April 2006, Office of Security Evaluations officials provided us plans for performing additional oversight inspections for the remainder of 2006. These plans included inspections evaluating classification activity at eight DOE offices at three additional sites. In addition, according to the Director of the Office of Security Evaluations, the procedures for conducting future oversight are still evolving—including the numbers of sites to be inspected and the depth of analysis to be performed. If the oversight inspections planned for the remainder of 2006 are completed, it will demonstrate resumption in the pace of oversight conducted prior to October 2005. However, if these inspections are not completed, or are not as comprehensive as they used to be, the extent and depth of oversight will be diminished and may result in DOE classification activities becoming less reliable and more prone to misclassification.

On the basis of reviews of classified documents performed during its 34 oversight inspections, the Office of Classification believes that very few of DOE's documents are misclassified, but we found that document selection procedures varied, and at times, may have limited the depth and independence of the document reviews. The department's review of more than 12,000 documents between 2000 and 2005 uncovered 20 documents (about one-sixth of 1 percent) had been misclassified. Most misclassified documents remained classified, just not at the appropriate level or category. Of greater concern are the several documents that should have been classified but mistakenly were not. When mistakenly not classified, such documents may end up in libraries or DOE Web sites where they could reveal classified information to the public. DOE officials believe that its misclassification rate is reasonable, given the large volume of documents processed. While DOE officials' goal is to classify all documents correctly, they recognize there is some element of subjectivity in classification decisions and that training, good guidance, and oversight are the best ways of ensuring the rate of misclassification is kept as low as possible. Until October 2005, the Office of Classification evaluated DOE's management of classified information by sending expert teams to sites and

program offices to draw and review nonprobability samples of thousands of pages of documents. At each site, Office of Classification inspectors reviewed documents and found that no site had more than five misclassified documents, and 25 sites had none. For example, during a review of classified documents at Los Alamos National Laboratory in New Mexico in May 2005, an Office of Classification team reviewed 314 classified documents, consisting of nearly 7,000 pages, 135 newly created unclassified documents consisting of over 3,000 pages, and nearly 6,500 pages on the publicly available Los Alamos Web site and linked Internet pages. Among the 314 classified documents, inspectors found that 4 documents were misclassified. These misclassifications included both overclassifying documents and underclassifying them. Among the 135 newly created unclassified documents, inspectors found a more serious error: a document in the Los Alamos technical library that was unclassified contained classified information on nuclear weapons. The only notable shortcomings we identified in how DOE conducted these inspections were the inconsistent way documents were selected for review and the failure to adequately disclose these selection procedures in their reports. At some sites, the team could make decisions on which documents to review on the basis of unfettered access to all classified document files; whereas at other sites, some files were not available for inspection; and still in other cases, the Office of Classification inspection team reviewed documents selected for it by site officials. Furthermore, Office of Classification reports did not disclose to the reader key facts about how information was gathered, what limitations the office agreed to, and how this affected its findings. Together these shortcomings may limit the independence of DOE oversight and potentially undermine confidence in the credibility of its findings.

We are making recommendations to help ensure that DOE classification activities remain effective and result in documents that are classified and declassified according to established criteria. Specifically, we recommend that the Secretary of Energy (1) ensure that the classified information oversight program provides oversight to a similar number of sites, as it had done prior to October 2005 and a similar depth of analysis; (2) strengthen the review of classified documents by applying consistent selection procedures when identifying documents for review; and (3) disclose the selection procedures used for document review in future classification inspection reports.

We provided a draft of this report to DOE for comment. DOE agreed with the report's recommendations, but commented that it was already taking actions and making plans to ensure that the classification oversight

program remains effective. Although we are encouraged by DOE's efforts, until the agency establishes a record of accomplishment under the new organizational structure, it will not be clear whether oversight will be as effective as it has been in the past.

Background

The U.S. government classifies information that it determines could damage the national security of the United States if disclosed publicly.[4] Currently, all classified information falls under two authorities, one for national defense and foreign relations, the other for nuclear weapons and technology. Beginning in 1940, classified national defense and foreign relations information has been created, handled, and safeguarded in accordance with a series of executive orders. Executive Order 12958, *Classified National Security Information*, as amended, is the most recent.[5] It establishes the basis for designating National Security Information (NSI). It demarcates different security classification levels, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage (Top Secret), serious damage (Secret), or damage (Confidential). It also lists the types of information that can be classified and describes how to identify and mark classified information. In 2005, about one quarter of DOE classification decisions concerned NSI.

The advent of nuclear weapons during World War II, led to a new category of classified information. In 1946, the Congress enacted the Atomic Energy Act, which established a system for governing how U.S. nuclear information is created, handled, and safeguarded.[6] Nuclear information

[4]In Executive Order 12958, as amended, "national security" means the national defense or foreign relations of the United States. In addition, the U.S. government also designates some information as "controlled." Controlled information is restricted from unauthorized disclosure. According to DOE officials, although it is less sensitive than classified information, it may be shared with people lacking security clearances provided officials determine they have a "need to know." There are four categories of controlled information at the DOE: (1) Unclassified Controlled Nuclear Information (UCNI), (2) Unclassified Naval Nuclear Propulsion Information (U-NNPI), (3) Official Use Only (OUO), and (4) Other Agency Controlled Information. For information about UCNI and U-NNPI, please see appendix I of this report. For information about DOE's management of OUO, see GAO-06-369.

[5]Executive Order 12958 was amended most recently by Executive Order 13292 on March 25, 2003.

[6]Pub. L. No. 79-585, 60 Stat. 755 (1946).

categorized as Restricted Data (RD) or Formerly Restricted Data (FRD)[7] is not governed by Executive Order 12958. RD is defined as data concerning the design, manufacture, or utilization of atomic weapons; production of special nuclear material; and use of special nuclear material in the production of energy. This includes information about nuclear reactors that produce plutonium and tritium, radioactive isotope separation techniques, and the quantities of nuclear materials involved in these processes. FRD relates primarily to data regarding the military use of nuclear weapons. Examples of FRD include weapons stockpile data, weapon yields, the locations of nuclear weapons, and data about weapons safety and storage. Like NSI, classified nuclear information also has three classification levels: Top Secret, Secret, or Confidential.

Naval Nuclear Propulsion Information (NNPI) is an exceptional category, which may fall under either of the two classification authorities. NNPI is deemed by both DOE and the Department of Defense (DOD) to be sufficiently sensitive to merit special protections and may be classified under the Atomic Energy Act or Executive Order 12958, depending on its subject and details.

Some Controlled Information Remains Unclassified

Two categories of nuclear information can be withheld from the public without being classified: Unclassified NNPI and Unclassified Controlled Nuclear Information (UCNI). Unclassified NNPI and UCNI are information the government considers sufficiently sensitive to withhold from public release, but not so sensitive as to warrant designation as RD, FRD, or NSI.[8] UCNI is a category created under the authority of the Atomic Energy Act, which enables DOE officials to share information with state and local law enforcement and emergency services personnel who, while lacking security clearances, may have a legitimate need to know operational details about, for example, planned shipments of special nuclear materials.

[7]The term "Formerly" means that the information is no longer classified as "Restricted Data," not that it is no longer classified. This determination is made jointly by DOE and the Department of Defense (DOD) when they conclude that the information is primarily operational in nature and can be adequately safeguarded as defense information.

[8]Unclassified NNPI is less sensitive than classified NNPI and must be protected in accordance with Navy regulations and under various export control requirements and statutes.

Documents Can Be Classified in Whole or in Part

According to the current executive order, documents containing only NSI must be "portion marked," for instance, classified paragraph-by-paragraph. For example, a document containing NSI may have paragraphs classified as Top Secret, Secret, or Confidential, along with others that are unclassified. However, documents containing any RD or FRD are classified in their entirety at the level of the most sensitive information in the document. Portion marking of documents containing RD and FRD is not required by the Atomic Energy Act and is discouraged by DOE policy.[9]

Requirements Vary for Declassifying Documents

Executive Order 12958, as amended, states that NSI shall be declassified as soon as it no longer meets the standards for classification.[10] The point at which information is to be declassified is set when the decision is made to classify it, and it is linked to an event, such as a completed mission, or to a period of time. Classified records that are older than 25 years and have permanent historical value are automatically declassified unless an exemption is granted because their contents still remain sensitive and their release could harm national security. Agencies have adopted processes to facilitate declassification in compliance with the executive order.

Unlike documents containing NSI, documents containing RD or FRD are not reviewed automatically for possible declassification.[11] The reason for this is that these two categories are mostly scientific and technical and may not become less sensitive with the passage of time. In fact, such data may be useful to nations and terrorist groups that are trying to build nuclear weapons. At a time of increased concern about nuclear proliferation, some of the oldest and simplest nuclear technology can be useful for making weapons of mass destruction. For this reason, documents about nuclear weapons and technologies from the 1940s and 1950s remain especially sensitive and worthy of protection.

[9]The Atomic Energy Act does not require portion marking on any documents containing RD or FRD information. DOE M 475.1-1A at VI-4,5, *Identifying Classified Information*, discourages portion marking of any documents containing RD or FRD information, even if the document also contains NSI, which would otherwise require it.

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

[11]While there is no specified time period for declassification of RD and FRD, DOE policy requires such information to be reviewed "continuously" to determine whether it may be removed from these categories, and DOE must review this information upon request. See DOE M 475.1-1A, IV-1—IV-4.

DOE Guidance on Classification

DOE implements the executive order and classification statutes by issuing departmental regulations, directives, and extensive use of classification guides. DOE's directive, *Identifying Classified Information*,[12] is the department's comprehensive guide to classifying, declassifying, marking, and protecting information, documents, and material. The directive also establishes policies and procedures, such as departmentwide training and certification requirements for staff authorized to classify or declassify information, and for periodic self-assessments. Classification guides are manuals specifying precisely which DOE information must be classified, how it should be categorized (NSI, RD, or FRD), and at what level (Top Secret, Secret, or Confidential) it should be protected. DOE has a detailed and comprehensive set of classification guides that are integral to efficient functioning of the department's classification activities. The department limits the use of "source documents" for the purpose of making classification decisions.[13] Source documents may be used to classify documents containing NSI, but only when there is no guidance available.[14] For example, if a DOE classifier is evaluating a new document with the same information found in another document already classified as Secret, then this new document may also be classified as Secret. RD and FRD documents can never be used as source documents.

[12]DOE M 475.1-1A, *Identifying Classified Information*, approved May 8, 1998. DOE officials expect a revised and updated order, DOE M 475.1-1B to be promulgated in July 2006.

[13]Executive Order 12958, as amended, defines "source document" as "an existing document that contains classified information that is incorporated, paraphrased, or generated in new form into a new document."

[14]DOE policy states that a source document can only be used to classify information as NSI when it is entirely under the purview of another U.S. government agency, a foreign government, or an international organization and no guidance exists.

DOE Training, Guidance, and Oversight Programs Have Been Effective over Time, but a Recent Change in Oversight Responsibility Has Created Uncertainty

DOE's Office of Classification's systematic training, comprehensive guidance, and rigorous oversight programs had a largely successful history of ensuring that information was classified and declassified according to established criteria. DOE's training requirements and classification guidance are essential internal controls that provide a strong framework for minimizing the risk of misclassification. However, since responsibility for classification oversight was shifted from the Office of Classification to the Office of Security Evaluations in October 2005, the pace of oversight was interrupted—creating uncertainty about how oversight will be performed and whether it will continue to be effective.

DOE's Classification Training and Guidance Programs Are Systematic and Comprehensive

Systematic training requirements are an important element of DOE's framework for maximizing the proper classification of documents. Only staff that have successfully completed training are authorized to classify or declassify documents. Staff must be recertified as classifiers and/or declassifiers every 3 years, in order to retain their authority. Staff are typically trained as "derivative classifiers" and, in some cases, as "derivative declassifiers" as well. They are limited in their authority to those areas in which they have special knowledge and expertise and are only authorized to classify (or declassify) documents "derivatively"—that is, only if the document in question contains information a DOE or other U.S. government agency classification guide specifically requires be classified or declassified.[15] There are currently about 4,600 derivative classifiers in DOE, nearly all of whom do classification work only as a collateral duty. For example, most derivative classifiers in DOE are scientists, engineers, or other technically trained people who work in programs or areas involving classified information that need staff who can properly classify the documents these programs produce. Relatively few DOE staff (just 215 as of May 2006) are authorized to declassify documents. Because a declassified document may become publicly available, derivative declassifiers are among the most experienced derivative classifiers. Only original classifiers, of which there are currently 25 throughout the DOE complex, are authorized to classify previously

[15]As previously discussed, source documents may also be used for documents containing classified NSI so long as they are under the purview of another agency and no other guidance is available.

unclassified information.[16] All DOE original classifiers are either very senior, full-time classification professionals, such as the director and deputy director of the Office of Classification, or one of the department's top-level political appointees, such as the Administrator, National Nuclear Security Administration.

DOE has developed an extensive collection of more than 300 classification guides, or manuals, specifying precisely which DOE information must be classified, how it should be categorized, and at what level (Top Secret, Secret, or Confidential) it should be protected. The Office of Classification oversees the regular updating of all classification guides used in DOE and must ultimately approve the use of every guide. DOE prohibits classification decisions based on source documents for documents containing RD and FRD and permits their use only when no guidance is available for documents containing NSI from other federal agencies. The Information Security Oversight Office considers the use of classification guides to be a best practice because they provide a singular, authoritative voice that is less open to individual interpretation or confusion than source documents and so using these guides are less likely to result in errors.[17] According to the Information Security Oversight Office, DOE's use of classification guides is among the most extensive in the federal government. Classification guides are integral to the efficient functioning of the department's classification program. Some classification guides are more general in nature, such as those dealing with physical security, and are used widely throughout DOE. Others, known as "local guides," are used at a few or even a single site because they provide guidance specific to a single DOE program or project. For example, a classification guide used by contractors working on a decontamination and clean-up project at a site in Oak Ridge, Tennessee, provides specific guidance on nuclear waste and storage unique to this site.

DOE has also implemented an extensive and rigorous oversight program. From 2000 through 2005, the Office of Classification and its predecessor offices have conducted on-site inspections of classification activities at 34

[16]In DOE, original classifiers are authorized to classify as NSI previously unclassified information. The original classification of information as RD or FRD is determined by regulations based on the Atomic Energy Act. Decisions to classify information as RD or FRD must also be approved by top managers in DOE's Office of Security and Safety Performance Assurance.

[17]The Information Security Oversight Office is responsible for policy and oversight of information classified under the authority of Executive Order 12958, as amended, as NSI.

DOE field offices, national laboratories, and weapons manufacturing facilities. In calendar years 2004 and 2005, the Office of Classification conducted an average of 10 oversight inspections a year. Classification activities were evaluated in depth in eight different functional areas, including site-provided classification training, self-assessment efforts, and overall senior management support for (and awareness of) classification activities. To this end, before a team of 3 to 10 Office of Classification inspectors arrived, it would send the site's classification officer a "data call" requesting detailed and specific answers to dozens of questions about the procedures and practices of the site's classification program. For example, to ascertain how effectively classification guidance was being used, requests were made for information about what guidance was in use at the site; the names of authorized classifiers who had guides; whether there were any local (site-specific) guides in use, and if so, when were they last validated by Office of Classification officials. Similarly detailed requests for information were requested about each of the other classification program elements. Having such detailed information in hand prior to arrival at the site allowed inspection teams to undertake a comprehensive evaluation in just 2 to 5 days because they could focus more on validating the information provided in the data call than on undertaking the time-consuming task of gathering data themselves. The Office of Classification staff's expertise in classification matters is augmented with subject area experts. For example, to ensure the inspection team had adequate expertise to make valid assessments of classification decisions about nuclear weapons design at Los Alamos National Laboratory, a staff member with nuclear weapons design experience was assigned to the team. Moreover, in many cases, members of the inspection team had more than 20 years of classification experience. As a result of the extensive information provided by the data call, and the level of experience of the inspection team, generally the team submitted a draft inspection report to the site's classification officer before leaving. It is DOE policy that any findings requiring immediate correction resulted in the creation of a corrective action plan, which had to be completed within 60 days of the inspection. DOE officials told us progress on implementing corrective action plans was reported to the Office of Classification quarterly.

In September 2005, the Information Security Oversight Office reviewed DOE's classification program just prior to the shift in responsibility for

classification oversight.[18] Officials at the Information Security Oversight Office found DOE's program to be much better than the average federal agency. They singled out DOE's training program and extensive use of classification guidance as especially impressive. One official called DOE's program for ensuring that all staff authorized to classify and declassify documents were recertified every 3 years "outstanding." Another official called DOE's extensive use of classification guides a "best practice." Overall, Information Security Oversight Office officials were impressed with DOE's classification program, noting that robust oversight is a very important part of an effective program for managing classified information.

Continued Effectiveness of Classification Oversight Is Uncertain

Since responsibility for classification oversight was shifted from the Office of Classification to the Office of Security Evaluations, the pace of oversight was interrupted—creating uncertainty about how oversight will be performed and whether it will continue to be effective. The Office of Security Evaluations is the DOE office responsible primarily for the oversight of physical security at DOE sites, with a special emphasis on Category 1 sites (sites containing special nuclear materials). Since October 2005, the Office of Security Evaluations has completed one inspection of two offices at the Pantex Site in Texas and another inspection of four offices at the Savannah River Site is under way. In April 2006, Office of Security Evaluations officials provided us plans for performing additional oversight inspections for the remainder of 2006. These plans included inspections evaluating classification activity at eight DOE offices at three additional sites. Classification oversight has been incorporated into larger oversight efforts on physical security at DOE sites.

Classification oversight ceased from October 2005 until February 2006 when the Office of Security Evaluations began its inspection of two offices at the Pantex Plant, a nuclear weapons manufacturing facility in Texas. Before the shift in responsibility, DOE officials did not conduct any risk assessment of the likely effects on the classification oversight program of the shift for three reasons: (1) they did not consider the shift to be a significant organizational or management challenge because the upper-

[18]The Information Security Oversight Office does not have the authority to evaluate how DOE manages RD or FRD—information classified under the authority of the Atomic Energy Act. Although only about one-quarter of DOE classification decisions concerned NSI in 2005, the policies and procedures governing the management of RD and FRD are essentially the same.

level management remained the same; (2) the Office of Security Evaluations would continue to draw on many of the same experienced Office of Classification staff who have been performing classification oversight for many years; and (3) responsibility for other key internal controls for managing classification activities, namely training and guidance, would remain with the Office of Classification. The director of the Office of Security Evaluations and the acting deputy director of the Office of Classification told us that the goal of shifting responsibility for classification oversight from one office to the other was to consolidate all oversight functions in one area. The idea arose in the course of a periodic reassessment of the organization of the Office of Security and Safety Performance Assurance—the larger organization of which these and several other offices are part—and a judgment by senior DOE management that one group should do all the oversight. The Office of Security Evaluations seemed the most logical place to locate classification oversight, according to senior DOE management. DOE officials also told us that the Office of Security and Safety Performance Assurance was not the only part of DOE affected by this drive to consolidate functions in single offices, and there was no intent to downgrade oversight.

According to the Director of the Office of Security Evaluations, the procedures for conducting future oversight are still evolving—including the numbers of sites to be inspected and the depth of analysis to be performed. The office currently plans to evaluate classification activities at 14 offices within five DOE sites in calendar year 2006, integrating classification oversight into its regularly scheduled inspections of Category 1 sites with inspections at a few non-Category 1 sites.[19] The director of the Office of Security Evaluations said the goal is to visit each of DOE's 10 Category 1 sites every 2 years. However, this schedule has been recently delayed as the office has been tasked by senior DOE management to perform security reviews in other areas of DOE operations. Now that classification oversight is a component within the much larger oversight agenda of the Office of Security Evaluations—one focused on the physical security of DOE's most sensitive sites—it raises uncertainty about whether classification oversight will have a diminished priority than when it was solely an Office of Classification responsibility. However, if all of the visits planned for 2006 are completed, then the Office

[19]These five sites include the Pantex Site, which has already been completed; the Savannah River Site, which is ongoing; Argonne National Laboratory, the Hanford Reservation, and Los Alamos National Laboratory.

of Security Evaluations will be conducting oversight at a pace similar to what was done prior to October 2005.

As classification oversight is now the responsibility of the Office of Security Evaluations—and will be reported as one component in a much larger report on the overall security of DOE sites—it is unclear if the new format will have the same depth of analysis or be as comprehensive, detailed, and useful as the format used by the Office of Classification. The Office of Security Evaluations reports are bigger and have a much higher profile with senior DOE management than reports by the Office of Classification. As such, they are written to convey information to a broader and less technically oriented audience. Each element of security is rated as "effective performance" (green), "needs improvement" (yellow), or "significant weakness" (red). To accommodate this shift, the format for reporting the results of inspections of classification activities has changed to fit into this larger, well-established Office of Security Evaluations reporting format. These reports have relatively brief executive summaries but are supplemented by several appendixes, one for each component of site security. The executive summary includes the highlights of the inspection, an overall evaluation of security at the site, the formal findings (that is, deficiencies uncovered), and a brief scope and methodology section (which includes a listing of the personnel participating in the inspection). It is uncertain if the results of the inspection of classification activities will be included in the executive summary, or if this depends on whether the results are particularly noteworthy. Not all aspects of an inspection will be mentioned in the summary section, and most of what is reported on classification and other topics will be in their respective appendixes. The Office of Security Evaluation's full report will be classified because it will contain information on the vulnerabilities in site security. However, according to the Office's director, the appendix on classification will likely be unclassified.

Since the shift in responsibility, the Office of Security Evaluations has completed one classification inspection of two offices at the Pantex Site; and the new procedures for oversight are still evolving. It is uncertain whether the reporting on classification oversight will be as detailed, specific, and, ultimately, as useful as it was prior to the October 2005 shift in responsibility. While the overall reporting format for the Office of Security Evaluations reports is firmly in place, the director of the office told us that the details of how to assess the effectiveness of the classification program is still evolving. Initially, the Office of Security Evaluations plans to gather similarly detailed and comprehensive information from the sites it inspects using the same "data call" as the

Office of Classification; the data call requests detailed and specific answers to dozens of questions about the procedures and practices of the site's classification program. The director of the Office of Security Evaluations stressed—and the deputy director of the Office of Classification agreed—that they plan to have the information reported in the classification appendix written in language similar to that in Office of Classification reports, and findings and recommendations for improvement will be conveyed in language no less specific and "actionable" than in the previous reports. Nonetheless, until the Office of Security Evaluations performs several classification inspections and establishes its own record of accomplishment in overseeing DOE classification activities, it is not clear whether oversight will be as effective as it was before the shift in responsibility. Without continued effectiveness, DOE classification activities could become less reliable and more prone to misclassification.

DOE Internal Reviews Found Very Few Documents Have Been Misclassified, but Document Selection Procedures Are Not Consistent and Lack Transparency

On the basis of reviews of over 12,000 classified documents totaling nearly a quarter million pages at 34 sites between 2000 and 2005, DOE officials have found that very few documents are misclassified. Office of Classification inspectors found 20 documents had been misclassified, an error rate of about one-sixth of 1 percent.[20] At more than two-thirds of the sites (25 of 34) inspectors found no classification errors. The most misclassified documents that these inspectors found at any site were five, at the Los Alamos National Laboratory in May 2005. Four of these documents were classified, but not at the proper level or category. A fifth document containing nuclear weapons information should have been classified but was unclassified and found in the laboratory's technical library. (See table 1.)

[20]DOE's document reviews are useful, but because DOE does not have a complete inventory of its classified documents, it cannot select a strictly random sample, and thus its findings are not generalizable.

Table 1: DOE Classification Reviews and Findings, 2000–2005

Site	Dates of review	Number of documents reviewed	Number of pages reviewed	Misclassifications	Percent of documents misclassified
Office of Science and Technical Information	Oct 2005	82	2,846	0	0
Y-12 Site Office	Oct 2005	83	1,525	0	0
Y-12 Complex	Oct 2005	575	11,347	0	0
Livermore Site Office	Aug 2005	1,112	7,064	3	0.27
Livermore National Lab	Aug 2005	222	5,382	3	1.35
Sandia National Lab/California	Aug 2005	187	3,850	0	0
NNSA Service Center	July 2005	840	5,439	0	0
Office of Secure Transportation	July 2005	64	763	0	0
Office of Civilian Radioactive Waste Management	June 2005	213	1,650	0	0
Los Alamos Site Office	May 2005	154	427	0	0
Los Alamos National Lab	May 2005	449	16,454	5	1.11
Office of the Assistant Secretary for Environmental Management	Mar-Apr 2005	25	375	0	0
Sandia Site Office	Mar 2005	12	1,110	0	0
Sandia National Lab/New Mexico	Mar 2005	174	11,153	2	1.15
Pantex Site Office	Nov 2004	52	680	0	0
Pantex Plant	Nov 2004	240	16,753	2	0.83
Kansas City Site Office	July 2004	14	94	0	0
Kansas City Plant	July 2004	29	682	0[a]	0[a]
Oak Ridge Operations Office	June 2004	634	17,353	1	0.16
Paducah Plant	Mar-Apr 2004	18	59	0	0
Portsmouth Plant	Mar 2004	13	680	0	0
Idaho Operations Office	Aug 2003	49	2,232	0	0
Livermore Site Office	June 2003	327	6,499	0	0
Richland Operations Office	Apr 2003	233	9,933	0	0
Savannah River Operations Office	Oct 2002	325	10,362	0	0
Rocky Flats Field Office	Jun 2002	567	10,905	1	0.18

Site	Dates of review	Number of documents reviewed	Number of pages reviewed	Misclassifications	Percent of documents misclassified
Office of Science and Technical Information	Oct 2005	82	2,846	0	0
Nevada Operations Office	Mar 2002	859	10,196	0	0
Oak Ridge Operations Office	June-July 2001	953	22,751[b]	0	0
Ohio Field Office	Apr 2001	225	1,642	1	0.44
Albuquerque Operations Office	Mar 2001	2,095	24,447[b]	0	0
Richland Operations Office	Nov 2000	334	11,510[b]	0	0
Oakland Operations Office	Sep-Oct 2000	248	1,214[b]	2	.81
Savannah River Operations Office	June 2000	182	4,173[b]	0	0
Nevada Operations Office	Mar-Apr 2000	581	4,100[b]	0	0
Total		**12,170**	**225,650**	**20**	**0.16**

Source: GAO analysis based on DOE data.

[a]The original report on the Kansas City Plant cited two misclassified documents. Subsequently, plant officials appealed this finding, and the Office of Classification agreed that the two documents in question were not misclassified.

[b]For these reviews, Office of Classification inspectors estimated the number of pages they analyzed.

Most misclassified documents remained classified, just not at the appropriate level or category. Of greater concern would be documents that should be classified but mistakenly are not. When mistakenly not classified, such documents may end up in libraries or on DOE Web sites where they could reveal sensitive RD and FRD to the public. When documents are not classified but should be, these errors can only be uncovered through some form of oversight, such as the document reviews that occurred in preparation for, and during, Office of Classification inspections. For example, during an inspection at the Sandia National Laboratories in March 2005, Office of Classification inspectors reviewed more than 170 unclassified documents in the laboratory's holdings and found 2 documents that contained classified information. Without systematic oversight, these kinds of errors are unlikely to be discovered and corrected.

While DOE's extensive document reviews provided depth and rigor to its oversight inspections, two notable shortcomings in this process were (1) the inconsistent way that inspectors gained access to the many documents

they would review and (2) the failure to adequately disclose these procedures in their reports. At the six DOE sites we visited, the procedures that the Office of Classification inspection teams used to obtain documents varied widely. For example, at the Los Alamos National Laboratory, inspectors were granted unfettered access to any storage vault and library, and they themselves chose the documents for review.[21] Once in the vault or library, inspectors used the document indexes or interviewed the librarians to decide which documents and topics were recently classified or declassified. The inspectors requested the documents of most interest, or they browsed in the collection and pulled files randomly from the shelves. By contrast, at the NNSA Service Center in Albuquerque, site officials selected documents from several different locations, and then inspectors chose from among them. By not being able to select their own samples, Office of Classification inspectors limited their independence—which could possibly undermine the credibility of their findings. Because DOE does not have a complete inventory of its classified documents, it cannot select a strictly random sample. Nonetheless, DOE officials acknowledged they could improve their selection procedures to make them more consistent and random. Furthermore, in the 34 inspection reports we analyzed, Office of Classification inspectors did not disclose to the reader key facts about how information was gathered, what limitations they agreed to, and how this affected their findings. According to *Standards for Internal Control in the Federal Government*,[22] independent inspections should properly document and report on the processes they use in their evaluations. The Office of Classification's reports provided no detail about how documents were chosen. Such detail would increase public confidence that DOE's classification oversight is transparent and robust.

Conclusions

Since the 1950s, the DOE's Office of Classification and its predecessor organizations have developed strong systems of internal controls for managing classified information. At the core of these systems are (1) DOE's requirement that staff authorized to classify documents must

[21]At Los Alamos, by agreement between laboratory officials and the Office of Classification review team, inspectors did not request the two most sensitive types of documents: those detailing how nuclear weapons can be controlled and detonated.

[22]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). This publication is supplemented by *Internal Control Management and Evaluation Tool*, GAO-01-1008G (Washington, D.C.: August 2001).

complete training and be periodically recertified, (2) its comprehensive guidance, and (3) its program of regular and rigorous oversight to ensure that DOE sites are following agency classification policies. These training, guidance, and oversight programs have provided a proven framework that has contributed to DOE's success in managing classified information. However, the recent reduction in oversight activity following a shift in responsibilities raises questions about whether this framework will continue to be as strong. If the oversight inspections planned for the remainder of 2006 are effectively completed, it will demonstrate resumption in the pace of oversight conducted prior to October 2005. However, if these inspections are not completed, or are not as comprehensive, then the extent and depth of oversight will be diminished and may result in DOE classification activities becoming less reliable and more prone to misclassification. In addition, by implementing more random selection procedures for identifying classified documents to review—and by disclosing these procedures clearly in their reports—DOE has the opportunity to assure both itself and the public that its oversight is, indeed, effective. DOE is the agency most responsible for safeguarding the nation's nuclear secrets, and its classification and declassification procedures are especially vital to national security. At a time when risks of nuclear proliferation are increasing, it is imperative that DOE build on its past successes in order to continue to be effective.

Recommendations for Executive Action

To help ensure that DOE classification activities remain effective and result in documents that are classified and declassified according to established criteria, we recommend that the Secretary of Energy take the following three actions:

- ensure that the classified information oversight program provides oversight to a similar number of DOE sites, as it did before October 2005, and provides a similar depth of analysis;
- strengthen the review of classified documents by applying selection procedures that more randomly identify documents for review; and
- disclose the selection procedures used for documents for review in future classification inspection reports.

Agency Comments and Our Evaluation

In commenting on the draft of this report, DOE agreed with the findings and recommendations of the report. DOE was pleased that its classification program is being recognized as particularly effective in

protecting information vital to national security. However, while DOE agreed with our recommendation that steps be taken to ensure that the classification oversight program provide oversight to a similar number of sites at a similar depth of analysis, it asserted that it is in fact already taking the needed actions and has, overall, "retained the effective framework previously established by the Office of Classification." Although we are encouraged by DOE's efforts, until the agency establishes a record of accomplishment under the new organizational structure, it will not be clear whether oversight will be as effective as it has been in the past.

DOE also concurred with our recommendations to strengthen the review of classified documents by applying selection procedures that more randomly identify documents for review and disclose these procedures in future reports and outlined steps it will take to implement these two recommendations.

Comments from DOE's Director, Office of Security and Safety Performance Assurance are reprinted in appendix II. DOE also provided technical comments, which we incorporated into the report as appropriate.

We are sending copies of this report to the Secretary of Energy; 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 me 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 that made major contributions to this report are listed in appendix III.

Sincerely yours,

Gene Aloise
Director, Natural Resources and Environment

Appendix I: Summary of DOE Classification and Control Policies

The Department of Energy (DOE) classifies and declassifies information under authorities granted by the Atomic Energy Act, first passed in 1946, and under presidential executive orders governing national security information. These authorities and corresponding implementing directives provide for three classification levels: Top Secret, Secret, and Confidential. DOE uses three categories to identify the different types of classified information: Restricted Data, Formerly Restricted Data, and National Security Information. In addition to classified information, certain types of unclassified information are sensitive and require control to prevent public release. The markings used and the controls in place depend on the statutory basis of the unclassified control system and vary in DOE, from Official Use Only information to Unclassified Controlled Nuclear Information. At a practical level, unclassified information is controlled or not controlled, depending on its sensitivity, any overriding public interest requiring release, or operational considerations involving the benefit of control versus the cost of control (for example, it must be shared with uncleared state or local government officials).

The information presented below is a summary of the various levels and categories used by DOE to classify and control information.

Levels of Classification

All classified information and documents are classified at one of three levels, listed in descending order of sensitivity: Top Secret (TS), Secret (S), or Confidential (C).

Categories of Classified Information

Restricted Data (RD)

- Classified under authority of the Atomic Energy Act (AEA) of 1954, as amended.
- Defined in the AEA[1] as all data concerning:
  - the design, manufacture, or utilization of atomic weapons; and
  - the production of special nuclear material. Examples include: (1) Production reactors (2) Isotope separation (gaseous diffusion, gas centrifuge, laser isotope separation).

[1]See 42 U.S.C. § 2014(y).

- The use of special nuclear materials in the production of energy. Examples include: (1) naval reactors, and (2) space power reactors.
- But not information declassified or removed from the RD category.

- Documents are not portion marked–an entire document is classified at the level of the most sensitive information contained in the document.[2]

Formerly Restricted Data (FRD)[3]

- Classified under authority of the AEA of 1954, as amended.
- Information that has been removed from the RD category because DOE and the Department of Defense have jointly determined that the information (1) now relates primarily to the military utilization of atomic weapons and (2) can be adequately safeguarded as defense information.[4] Examples include:
  - weapon stockpile quantities,
  - weapons safety and storage,
  - weapon yields, and
  - weapon locations.
- Documents are not portion marked.

National Security Information (NSI)

- Classified under the authority of Executive Order 12958, as amended.
- Information that pertains to the national defense or foreign relations of the United States and classified in accordance with the current executive order as Top Secret, Secret, or Confidential.
  - NSI documents may be classified up to a 25 year limit unless containing information that has been approved for exemption from declassification under Executive Order 12958, as amended, and based on an approved declassification guide.
  - For example, DOE treats certain nuclear-related information that is not RD or FRD, such as security measures for nuclear facilities, as exempt from declassification until such facilities are no longer in use. Many of these facilities have been in use for over 50 years.
- Documents are portion marked by paragraph.

[2]See DOE M 475.1-1A.

[3]Categorizing information as "Formerly Restricted Data" may be confusing because it implies to some that the information is no longer restricted or classified. It is "Formerly Restricted Data" in the literal sense: it is still-classified information that was formerly "Restricted Data."

[4]See U.S.C. § 2162(d).

- Confidential Foreign Government Information – Modified Handling Authorized (C/FGI-MOD)

An agency must safeguard foreign government information under standards providing a degree of protection at least equivalent to that required by the government or international organization that furnished the information. If the FGI requires a level of protection lower than that for Confidential, the United States can, under Executive Order 12958 section 4.1(h), classify and protect it as C/FGI-MOD, which provides protection and handling instructions similar to that provided to United States Official Use Only. Before C/FGI-MOD was created, the only legal way for such information to be controlled was at the Confidential level, which resulted in over-protection, increased security cost, and operational complexity.

Classification Markings

Each classified document must be marked to show its classification level (and classification category if RD or FRD), who classified it, the basis for the classification, and the duration of classification (if NSI).[5] Lack of a category marking indicates the classified document is NSI. A document containing only NSI must be portion marked.

- An RD document, for example, will be marked TSRD (Top Secret Restricted Data), showing the classification level and category. RD documents are similarly marked SRD (Secret Restricted Data), or CRD (Confidential Restricted Data). A document should never simply be marked "RD." The same rules apply to FRD information (TSFRD, SFRD, and CFRD).
- A classified document that is not RD or FRD is an NSI document. NSI documents are marked as TSNSI (Top Secret National Security Information), SNSI (Secret National Security Information), or CNSI (Confidential National Security Information); or simply Top Secret, Secret, or Confidential.

[5] See DOE M 475.1-1A.

Unclassified but Controlled Information (UCI)

Unclassified Controlled Nuclear Information (UCNI)

- Controlled under authority of the AEA of 1954, as amended.[6]
- Information concerning:
  - the design of nuclear material production facilities or utilization facilities;
  - security measures for protecting such facilities, nuclear material contained in such facilities, or nuclear material in transit;
  - The design, manufacture, or utilization of any atomic weapon or component if it has been declassified or removed from the RD category.
- UCNI markings – A document containing UCNI must be marked at the top and bottom of each page with "Unclassified Controlled Nuclear Information" or "UCNI" and include, on the front of the document, a marking that identifies the Reviewing Official making the determination, the date of the determination, and the guidance used.

Official Use Only (OUO)[7]

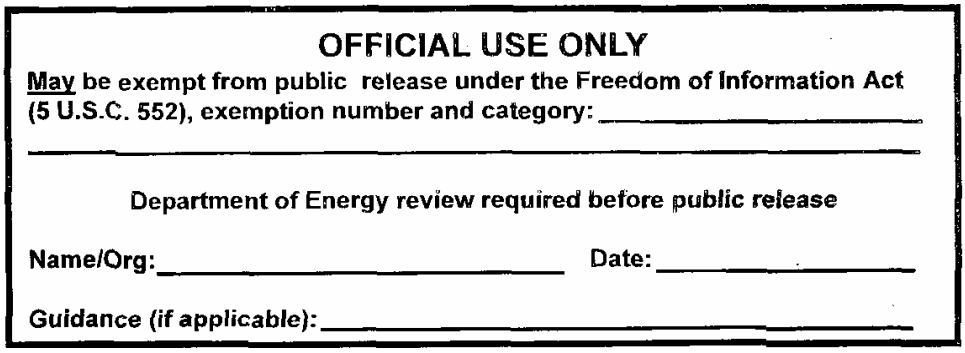
- Unclassified information that may be exempt from public disclosure under provisions of the Freedom of Information Act (FOIA) that is not otherwise subjected to a formally implemented control system.
- A decision to control information as OUO does not mean that such information is automatically exempt from disclosure if requested under the FOIA. That determination is made by a FOIA Authorizing Official only when the document is requested. The OUO marking merely serves as a warning that the document reviewer considers the information to be sensitive and indicates why by including on the document the FOIA exemption that the document reviewer thinks applies.
- OUO markings – Documents determined to contain OUO information are marked "Official Use Only" at the bottom of each page and include a marking on the front of the document that gives the name and title of the document reviewer making the determination, that document reviewer's determination of which FOIA exemption he or she believes applies, and a citation to the guidance relied upon, if any. (Note: Sometimes classification guides designate information as OUO rather than classified,

[6]See 42 U.S.C. § 2168.

[7]Official Use Only information is the subject of another GAO report; see GAO-06-369.

and when they do, they state which FOIA exemption applies. This classification guide is then cited on the OUO stamp.)

Figure 1: DOE's OUO Stamp



Source: DOE.

Naval Nuclear Propulsion Information (NNPI)

NNPI concerns all classified and controlled unclassified information related to the naval nuclear propulsion program. This marking supplements existing classification and control systems and is not a separate category outside of the authorities provided under the AEA or Executive Order 12958 for, as an example, classified NNPI. The use of "NNPI" is an additional marking applied to some of the previously defined categories of information to indicate additional controls for protection or access.

Classified Naval Nuclear Propulsion Information (C-NNPI)

- Classified under the authority of the AEA of 1954, as amended, or Executive Order 12958, as amended.
- All classified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of propulsion plants of naval nuclear powered ships and prototypes, including associated shipboard and shore-based nuclear support facilities.
- Markings can be RD or NSI.
  - C-NNPI documents containing RD information are marked TSRD, SRD, or CRD.
  - C-NNPI NSI documents are typically marked Secret NOFORN ("not releasable to foreign nationals"), or Confidential NOFORN. The NOFORN marking is used to indicate documents that should not be released to foreign entities.

    Note: There is no Top Secret NOFORN in the current Naval Reactors classification guidance.

- Documents containing information classified under the authority of the AEA are not portion marked.

Unclassified Naval Nuclear Propulsion Information (U-NNPI)

- Controlled in accordance with Naval Sea Systems Command Instruction C5511.32B and protected pursuant to export control requirements and statutes.
- All unclassified but controlled information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of propulsion plants of naval nuclear powered ships and prototypes, including associated shipboard and shore-based nuclear support facilities.[8]
- U-NNPI documents will be marked and controlled as NOFORN (not releasable to foreign nationals).

[8]See DOE M 470.4-4.

Appendix II: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

June 15, 2006

Mr. Gene Aloise
Director
Natural Resources and Environment
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-06-785, MANAGING SENSITIVE INFORMATION: Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System. The DOE is pleased that the classification program is recognized as one of the best in the Federal Government. As noted in your draft report, the DOE's systematic training, comprehensive guidance, and rigorous oversight ensure that our program is effective in protecting information vital to the national security.

While the DOE agrees with the three recommendations made in the report, we would like the opportunity to address the first one concerning the uncertainty of continued classification oversight of DOE sites. Despite the recent shift in responsibility to the Office of Security Evaluations, the classification oversight program has maintained a high level of performance, both in quantity and quality.

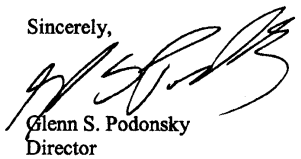
Since the Classification and Information Control oversight program was transferred to the Office of Security Evaluations, six organizations have been inspected and eight more are scheduled for inspection in 2006. These eight remaining inspections have been formally announced and placed on the schedule. Additionally, six of the eight organizations are not Category I sites and will be evaluated by the Classification and Information Control team only. This schedule demonstrates that the oversight program under the Office of Security Evaluations maintains the flexibility to conduct oversight inspections separate from the much larger physical security inspections that focus on Category I sites. This scheduling flexibility ensures that all sites with classification activities are evaluated on a periodic basis and reinforces our view that classification oversight remains a priority within the DOE.

Further, the DOE is committed to retaining the depth of analysis and comprehensive approach to the classification oversight program. One indicator of our commitment, included in the report, is the continuation of the data call that was used previously, which collects detailed information for an extensive review of an organization's classification

program. Another indicator is the continued support of experienced oversight personnel from the Office of Classification, which ensures continuity of inspection methods and procedures.

The DOE has retained the effective framework previously established by the Office of Classification. We continue to improve the appraisal protocols through constant and rigorous assessment of procedures and adaptation of better, more efficient methods. The DOE is committed to ensuring that the classification oversight program remains effective and one of the best in the Government.

Sincerely,



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

cc: M. Kilpatrick, SP-1
L. Gasperow, SP-1.2
J. Hawthorne, SP-50
A. Weston-Dawkes, SP-50
D. Williams, CF-1.2

DOE Response to GAO Draft Report
MANAGING SENSITIVE INFORMATION:
Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System (GAO-06-785)

In summary, the DOE finds the draft report to be a fair and accurate evaluation of its classification system. The DOE plans the following specific actions related to recommendations in the draft report:

Recommendation 1. We recommend that the Secretary of Energy ensure that the classified information oversight program provides oversight to a similar number of DOE sites as it did before October 2005, and provides a similar depth of analysis.

DOE Response. The DOE has already inspected six organizations and has formally announced plans to inspect eight other organizations in 2006. This schedule demonstrates that the pace in oversight has not slowed and that classification oversight remains a high priority for the DOE.

Additionally, the DOE is committed to maintaining the depth of analysis in the classification oversight program by adhering to the successful framework developed before October 2005. Effective methods such as the pre-inspection data call and the inclusion of classification experts on the inspection team are still being used to ensure a comprehensive approach. Appraisal methods are continuously evaluated for improvement.

Recommendation 2. We recommend that the Secretary of Energy strengthen the review of classified documents by applying selection procedures that more randomly identify documents for review.

DOE Response. The DOE plans to revise the selection process for document reviews during oversight inspections.

In the past year we have developed a standard procedure for selecting documents for review during oversight inspections. We based our selection criteria on factors such as (1) location, volume, and sensitivity of record collections; (2) security incident reports involving document review errors; and (3) document review results from previous inspections.

In addition, we are currently evaluating different sampling methods in order to ensure that the document selection process we adopt is consistent and effective and focuses on criteria that will yield random, statistically valid samples for our document review team to inspect.

Recommendation 3. We recommend that the Secretary of Energy disclose the selection procedures used for documents for review in future classification inspection reports.

DOE Response. The DOE plans to include the procedures used to select the documents reviewed during oversight inspections in future classification inspection reports.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Gene Aloise (202) 512-3841 or aloisee@gao.gov

Staff Acknowledgments

In addition, Nancy Crothers, Robin Eddington, Doreen Feldman, William Lanouette, Greg Marchand, Terry Richardson, Kevin Tarmann, and Ned Woodward made significant 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