TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

MEMORANDUM

To: Members of the Subcommittee on National Security, Emerging Threats, and International Relations

From: Christopher Shays
Chairman CS

Date: March 9, 2006

Subject: Briefing memo for the March 14th Subcommittee hearing

---

Attached find the briefing memo required by Committee rules for the hearing scheduled for Tuesday, March 14, 2:00 p.m. entitled, *Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information*. The hearing will convene at 2:00 p.m., room 2154 Rayburn House Office Building.

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

MEMORANDUM

To: Members of the Subcommittee on National Security, Emerging Threats, and International Relations

From: J. Vincent Chase

Subject: Briefing Memorandum for the hearing, *Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information*, scheduled for Tuesday, March 14, 2:00 p.m., 2154 Rayburn House Office Building.

Date: March 9, 2006

PURPOSE OF THE HEARING

The purpose of this hearing is to examine current practices for handling sensitive information and recommendations to prevent the overuse of classifications and other access restrictions.

HEARING ISSUES

1. To what extent do current policies and procedures on classification, declassification, reclassification and designation of *Sensitive but Unclassified* (SBU) and *For Official Use Only* (FOUO) material impede post-9/11 efforts to improve information sharing?

2. How effective are DOD and DOE policies and practices for the management of *For Official Use Only* information?

BACKGROUND

Since 1940, classification, declassification and reclassification of sensitive information have been governed by policies and procedures flowing from executive orders of the President. **(Attachment 1)** Successive executive directives reflect Cold War counterespionage concerns as well as persistent tension between the need for secrecy and public access to government information **(Attachment 2)**. By varying degrees, Presidents sought to protect national secrets through broader or narrower delegation of classification authority, by expanding or contracting categories of classifiable information and by endorsing or opposing the use of automatic declassification deadlines.

The first post-Cold War policy on classification was issued by President Clinton in 1995. Executive Order (EO) 12958 **(Attachment 3)** reset previous default settings, directing classifiers *not* to shield information of doubtful value and to classify information at the *lowest* rather than the highest possible level. With some exceptions, the order sets a ten year limit on classification markings and provides broadened opportunities for declassification of official materials. Reclassification was prohibited if the material had otherwise been properly put in the public domain. A new Interagency Security Classification Appeals Panel was established to make final decisions on certain classification challenges and declassification exemptions. **(Attachment 1, p5)**

Security concerns after the September 11th attacks prompted some departments and agencies to increase the type and volume of information shielded from public view by *Confidential*, *Secret* or *Top Secret* markings. In addition, President Bush issued E.O. 13292 **(Attachment 4)** amending E.O. 12958 that reverts to a "when in doubt, classify" standard, expands classification authorities and categories, created an automatic declassification program, and reinstituted reclassification. Moreover, it is not the case that the federal government uses only the three-tier *Confidential*, *Secret* or *Top Secret* classification process. In reality, the federal government has many varieties of sensitive material designations commonly referred to as sensitive but unclassified or SBUs.

The National Archives and Records Administration, Information Security Oversight Office (ISOO) oversees security classification programs for both government and government contractors and reports to the President annually on their status. A primary ISOO goal is to "provide for an informed American

public by ensuring that the minimum information necessary to the interest of national security is classified and that information is declassified as soon as it no longer requires protection."[1]

According to the latest ISOO annual report, in FY 2004 the combined classification activity of all government departments and agencies totaled 15,645,237 decisions, a 10 percent increase over what was reported for fiscal year 2003.[2] The total cost estimates for security classification within government for FY 2004 was $7.2 billion. The estimate of total security classification costs for 2004 for government contracts was $823 million.[3]

According to the ISOO, there are approximately 4,000 officials with original classification authority. They are the only individuals in the classification process authorized to exercise discretion in making classification decisions. While original classification authorities play a critical role in the first step of classification, it is derivative classifiers who make 92 percent of all classification decisions. They do this when they extract or paraphrase information in already classified materials or use their own interpretation of what they believe requires classification when consulting overly generalized classification guidelines. Derivative classifiers must be able to trace the origins of every act of derivatively classifying information to an explicit decision by a responsible official who has been expressly delegated original classification authority.[4]

Sensitive but Unclassified (SBU) Designations

According to the Wall Street Journal, sensitive information can be designated sensitive but unclassified and marked *For Official Use Only* by almost any government employee who concludes the information maybe exempt under the Freedom of Information Act.[5] **(Attachment 5)**

According to the Government Accountability Office (GAO), sensitive but unclassified designations refer to "information generally restricted from public

[1] National Archives, Information Security Oversight Office, Annual Report, FY 2004, http://www.archives.gov/isoo/reports/
[2] Ibid.
[3] National Archives, Information Security Oversight Office, *Annual Cost Report*, FY 2004, http://www.archives.gov/isoo/reports/2004-cost-report.pdf
[4] National Archives, Information Security Oversight Office, http://www.archives.gov/isoo
[5] Wall Street Journal, *Information Incognito*, Robert Block, March 22, 2005.

disclosure but that is not classified."[6] The designation of information as sensitive but unclassified has significantly increased since 9/11, reviving the debate over the objectivity of information security standards and the potential for excessive, abusive or politically motivated designations. While federal agencies used classification categories to withhold information pursuant to Executive Order 12958, federal agencies also use a variety of administrative control markings and procedures to control access to unclassified information to which public access is restricted, such as privacy data, law enforcement information, health information, business proprietary information, and other information exempt from disclosure under the Freedom of Information Act (FOIA).

Table 1: FOIA Exemptions

Exemption	Examples
1. Classified in accordance with an executive order*	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

Sharman, FOIA and Rich Jaroslovsky

According to CRS, at least 52 different protective markings are used on sensitive unclassified information. Included among these are widely-used markings such as *Sensitive but Unclassified*, *Limited Official Use*, *Official Use Only*, and *For Official Use Only*.[7] Other notable categories are *DHS Critical Infrastructure Information*, *Law Enforcement Sensitive*, and *DOD Unclassified Controlled Nuclear Information*. **(Web Resource 2, pg. 16)**

[6] General Accountability Office, GAO_05-667, *Transportation Security Administration: Clear Policies and Oversight Need for Designation of Sensitive Security Information*, June 2005.
[7] Moynihan Report on Government Secrecy, Web Site: www.fas.org/sgp/library/moynihan

During the hearing scheduled for March 14[t], the Subcommittee will release the GAO report entitled, *MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved.* The Subcommittee asked GAO to examine current Department of Defense (DOD) and Department of Energy (DOE) practices for handling SBU information and make recommendations to prevent the overuse of SBU access restrictions. **(Attachment 6)**

Department of Defense Use of SBU

DOD's guidance for "controlled unclassified information," issued in 1997, states "*For Official Use Only* (FOUO) designations should be used for unclassified information that should be protected, this includes information that may be exempt from mandatory release to the public under the Freedom of Information Act and that there must be a legitimate government purpose served by withholding it."[8] **(Attachment 7)**

This DOD directive restricts dissemination of information labeled FOUO including SBU information to only DOD components and between officials of DOD components, DOD contractors, and consultants in the conduct of official business. FOUO information may also be released to officials in other departments and agencies of the executive and judicial branches in performance of a valid government function. Release of FOUO information to Members of Congress is covered by DOD Directive 5400.4 and to the General Accounting Office by DOD Directive 7650.1. **(Web Resource 2, pg. 19)**

According to CRS, since there is no one source for a definition of SBU, other factors such as risk management, consideration of the effects of unauthorized disclosure, and an examination of the timeliness of information, should be taken into account as well. Ultimately, the level of sensitivity of the information should be determined by the owner or creator of the data. The following DOD matrix[9] **(Web Resource 2, pg. 19-20)** guides the definition of SBU information:

---

[8] Appendix 3C, Controlled Unclassified Information," In DOD 5200.1-R, *Information Security Program*, Jan. 1997, issued by Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

[9] Stuart D. Smith, "Sensitive But Unclassified Data; Identification and Protection Solutions, "Prepared for the U.S. Army Material Command Information Assurance Program Manger, July 2002, pg. 4-5.

Data Category	**Description**
FOIA Exempted	Any information that is exempted from mandatory disclosure under the Freedom of Information Act.
Intelligence Activities	Information that involves or is related in intelligence activities, including collection methods, personnel, and unclassified information.
Cryptologic Activities	Information that involves encryption/decryption of information; communications security equipment, keys, algorithms, processes; information involving the methods and internal workings of cryptologic equipment.
Command and Control	Information involving the command and control of forces, troop movements.
Weapon and Weapon Systems	Information that deals with the design, functionality, and capabilities of weapons and weapon systems both fielded and un-fielded.
RD&E	Research, development, and engineering data on un-fielded products, projects, systems, and programs that are in the development or acquisition phase.
Logistics	Information dealing with logistics, supplies, materials, parts and parts requisitions, including quantities and numbers.
Medical Care/HIPAA	Information dealing with personal medical care, patient treatment, prescriptions, physician notes, patient charts, x-rays, diagnosis, etc.
Personnel Management	Information dealing with personnel, including evaluations, individual salaries, assignments, and internal personnel management.
Privacy Act Data	Information covered by the Privacy Act of 1974 (5 U.S.C. § 552A)
Contractual Data	Information and records pertaining to contracts, bids, proposals, and other data involving government contracts.
Investigative Data	Information and data pertaining to official criminal and civil investigations such as investigator notes and attorney-client privileged information.

Source: "Sensitive But Unclassified Data; Identification and Protection Solutions, "Prepared for the U.S. Army Material Command Information Assurance Program Manger, Stuart D. Smith, July 2002

Department of Energy Use of SBU

According to CRS, the Department of Energy (DOE) defines sensitive but unclassified material as information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the government. National Security interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial,

agriculture, technological, and law-enforcement information, as well as the privacy or confidentially of personal or commercial proprietary information provided to the government by citizens. **(Web Resource 2, pg. 20)**

According to GAO, the Department of Energy Official Use Only (OUO) program was created in 2003. The program uses the exemptions in the Freedom of Information Act for designating information as OUO. The program provides guidance on how and when to identify information as OUO and eliminates various additional markings, such as "Patent Caution" or "Business Sensitive," for which there was no law, regulation or DOE directive to inform staff how such documents should be protected. **(Attachment 6)**

Reclassification of National Security Information

Declassification is an integral part of the security classification system. It is the authorized change in status of information from classified to unclassified. When Executive Order 12958 was issued on April 17, 1995 **(Attachment 3)**, there was a paradigm shift in declassification policies. In preceding years, information once classified remained so indefinitely and very often did not become available to the general public, researchers, or historians without persistent and continuous efforts on the part of those individuals. E.O. 12958 changed this paradigm by adding a new "Automatic Declassification" program **(Attachment 3, pg. 9)**.

The media reported recently that more than 55,000 pages of information previously declassified have been restored to classified status since 1999. **(Attachment 8)** Executive Order 12958 prescribes a uniform system for classifying, safeguarding, declassifying and reclassifying sensitive information, including information relating to defense against transnational terrorism. Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions outlined in EO 12958:

> (1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;
>
> (2) the information may be reasonably recovered; and

(3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. **(Web Resource 1)**

DISCUSSION OF HEARING ISSUES

To what extent do current policies and procedures on classification, declassification, reclassification and designation of *Sensitive but Unclassified* (SBU) and *For Official Use Only* (FOUO) material impede post-9/11 efforts to improve information sharing?

On July 22, 2004, the National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission) issued their final report. According to the 9/11 Commission, "secrecy stifles oversight, accountability and information sharing. Unfortunately, all of the current organizational incentives encourage overclassification. A system of 'need to know' should be replaced by a system of 'need to share'." **(Web Resource 3)** The Commission reported "security requirements nurture overclassification and excess compartmentation of information among agencies. Each agencies incentive structure opposes sharing, with risks including criminal, civil and administrative sanctions but few rewards for sharing information."

Many believe it has taken too long to change this culture of overclassification. Others argue September 11th has become an excuse for secrecy rather than a reason for it. One witness who testified before the Subcommittee in August 2004 stated, "the national security classification policy is erratic, undisciplined and prone to abuse.[10]" In January 2005, the GAO

[10] Prepared Statement of Steven Aftergood, Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, *TOO MANY SERECT: Overclassification As a Barrier to Critical Information Sharing*, Serial No. 108-263, pg. 43, August 24, 2004.

reported many aspects of homeland security information sharing remain ineffective and fragmented. In December 2005, 10 members of the former 9/11 Commission issued a report card outlining the government's progress in carrying out their recommendations regarding overclassification and information sharing. The members of the commission gave improving information sharing a grade of *D*. According to the commission members, changes to incentives in favor of information sharing have been minimal. The office of the program manager for information sharing is still a startup and is not getting the support it needs from the highest levels of government.

Some have argued that the increase in classification of information and the designation of *Sensitive but Unclassified* (SBU) and *For Official Use Only* (FOUO) material is the result of E.O. 13292 which reverted to the "when in doubt, classify" standard, expanded classification authorities and categories, and reinstituted reclassification from the 1995 standard.[11] In addition, in March 2002, the White House issued a memo **(Attachment 9)** to all agencies concerning the need to safeguard sensitive but unclassified information because such undefined information did not qualify for classification on national security grounds and explaining possible FOIA exemptions that could be used to withhold such information.

The balance between security and open government has never been easy, and it has gotten murkier since September 11th, which provided a rationale for agency officials to scour the public record for any information that had the potential to threaten national security.[12] To some it appears this examination now includes classifying information that had previously been declassified.

Others argue that the government's information policy is a state of near chaos, noting there is no consistency in dealing with SBU information not only with the public but with federal contractors and among government agencies. **(Attachment 10)** The Office of National Intelligence echoed this concern stating, 'the existence of multiple SBU designations, governed by its own unique set of procedures, adds a layer of complexity to efforts to share information." **(Attachment 10)**

---

[11] Prepared Testimony of Harry Hammitt, Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, *Emerging Threats: Overclassification and Pseudo-classification*, Serial No. 109-18, pg. 131-132, March 2, 2006.

[12] Congressional Quarterly, July, 18, 2005.

On December 16, 2005, the White House issued a memorandum **(Attachment 11)** "to promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of sensitive but unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information must be standardized across the federal government," Agencies were directed to assess their procedures for handling SBU and report on them to the Director of National Intelligence (DNI) within 90 days. Within a year, the DNI, with other agency heads, is to present recommendations for the President's approval on standardized SBU procedures. However, according to some, the White House directive does not acknowledge the reality that agencies often consider information sensitive for political or bureaucratic reasons unrelated to legitimate security or privacy concerns. Nor does the new memorandum consider that some kinds of admittedly sensitive information should nevertheless be publicly disclosed to promote government efficiency and accountability.[13]

How effective are DOD and DOE policies and practices for the management of *For Official Use Only* information?

The Department of Energy (DOE) and the Department of Defense (DOD) use the designations *Official Use Only* (OUO) and *For Official Use Only* (FOUO), respectively, to identify information that is unclassified but sensitive. According to GAO, there is no list of OUO or FOUO documents maintained by the agencies. Both DOE and DOD have offices, policies, and guidelines for designating sensitive but unclassified information. However, GAO found the policies governing DOE OUO and DOD FOUO programs allow for inconsistencies and errors.

According to GAO, 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, GAO found that DOD policy was unclear regarding which DOD office is responsible for the FOUO program. In 1998, the responsibility for the FOUO program was moved from the office of the Director of Administration to the

[13] Secrecy News from the FAS Project on Government Secrecy, Volume 2005, Issue No. 116, December 20, 2005.

Office of the Under Secretary of Defense for Intelligence. This change was not reflected in regulation and as a result guidance for the DOD FOUO program is included in the regulations issued by both offices. As a result, there is a lack of clarity regarding which DOD office has the primary responsibility for the FOUO program.

GAO also found DOE and DOD policies are unclear regarding when a document should be marked as OUO or FOUO. According to GAO, DOE policy is vague concerning the appropriate time to apply an OUO marking. DOE officials in the Office of Classification stated their policy does not provide specific guidance concerning when to mark a document OUO 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.

Some argue that the Department of Defense mindset is that all department information is for official use only. The Department of Defense, unlike the Department of Energy, has no department-wide requirement to indicate which FOIA exemption may apply to sensitive information because DOD has two regulations for determining how unclassified but sensitive information should be identified, marked, handled, and stored. GAO did find 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 GAO's view, if DOD were to require employees to take the extra step of marking the FOIA exemption at the time of document creation, it would help assure that the employee marking the document has at least considered the FOIA exemptions and made a thoughtful determination that the information fits within the framework of the FOUO designation. If a document is not marked at creation, but might contain information that is OUO or FOUO and should be handled as such, it creates a risk that the document could be mishandled.

GAO is recommending DOD revise the regulations to make it clear which office has the responsibility for the FOUO program and require personnel designating a document as FOUO to mark the document with the FOIA exemption used to determine the information should be restricted.

In addition, GAO found both DOE and DOD lack clear language identifying examples of inappropriate use of OUO or FOUO markings. According to *Standards for Internal Control in the Federal Government* **(Web Resource 4)**, agencies should have sufficient internal controls in place to mitigate risk and assure that employees are aware of what behavior is acceptable and what is unacceptable. Without explicit language identifying inappropriate use of OUO or FOUO markings, DOE and DOD cannot be confident that their personnel will not use these markings to conceal mismanagement, inefficiencies, or administrative errors or to prevent embarrassment to themselves or their agency.

GAO is recommending that DOE and DOD clarify by directive at what point a document should be marked as OUO or FOUO and to define what would be an inappropriate use of OUO or FOUO designations.

Finally, GAO found DOE and DOD offer training to staff on managing OUO and FOUO information. However, neither agency requires training before employees are allowed to identify and mark information as OUO or FOUO. In addition, neither DOE nor DOD has implemented an oversight program to determine the extent to which employees are complying with established policies and procedures. DOE and DOD officials stated that limited resources, and in the case of DOE, the newness of the program, have contributed to the lack of training requirements and oversight.

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

WITNESS TESTIMONY

PANEL ONE

Ms. Davi M. D'Agostino, Director, Government Accountability Office will testify about GAO findings and recommendations concerning DOD and DOE policies and practices for the management of *For Official Use Only* information.

Professor Allen Weinstein, Archivist of the United States, National Archives and Records Administration (NARA) will testify about the reclassification of records previously declassified and what actions NARA is taking to insure these records have been properly reclassified.

Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration will testify about documents that are wrongly reclassified and make recommendation about revising the reclassification program.

Mr. Robert Rogalski, Acting Deputy Under Secretary of Defense, Counterintelligence and Security will testify about GAO findings concerning DOD policies and practices for the management of *For Official Use Only* information and what DOD's intentions are for implementing GAO's recommendations that address those concerns.

Mr. Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, Department of Energy will testify about GAO findings concerning DOE policies and practices for the management of *For Official Use Only* information and what DOE's intentions are for implementing GAO's recommendations that address those concerns.

PANEL TWO

Mr. Thomas Blanton, Executive Director, National Security Archive, George Washington University will testify about the government's policy regarding the reclassification of records previously declassified.

Dr. Anna Nelson, Distinguished Historian in Residence, American University will testify about the government's policy regarding the reclassification of records previously declassified.

Mr. Matthew Aid will testify about the government's policy regarding the reclassification of records previously declassified.

ATTACHMENTS

1. CRS Report, *Security Classification Policy and Procedures: E.O. 12958, as Amended*, 97-771, January 7, 2005.

2. Executive Order 12356, *Uniform System for Classifying, Declassifying, and Safeguarding National Security Information*, April 2, 1982.

3. Executive Order 12958, *Classified National Security Information*, April 17, 1995.

4. Executive Order 13292, *Further Amendment to Executive Order 12958, As amended, Classified National Security Information*, March 25, 2003.

5. The Freedom of Information Act, as Amended, 5 U.S.C. 552.

6. *MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved*, Government Accountability Office, Report No. GAO-06-369, February 2006.

7. Appendix 3C, *Controlled Unclassified Information*, In DOD 5200.1-R, *Information Security Program*, Jan. 1997, issued by Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

8. *U.S. Reclassifies Many Documents in Secret Review*, New York Times, Scott Shane, February 21, 2006.

9. The White House, *Memorandum for the Heads of Executive Departments and Agencies*, December 16, 2005.

10. *Government Withholds 'Sensitive-but-Unclassified' Information*, Scripps Howard News Service, Lance Gay, February 2, 2006.

WEB RESOURCES

1. Executive Order 13292, Amending Executive Order 12958
http://www.fas.org/sgp/bush/eoamend.html

2. Congressional Research Service, Report No. RL31845, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: Background on the Controversy*, Updated February 20, 2004.
http://www.congress.gov/erp/rl/pdf/RL31845.pdf

3. The National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, July 22, 2004.
http://www.9-11commission.gov/report/911Report_Exec.pdf

4. Government Accountability Office, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1, November, 1999.
http://www.gao.gov/special.pubs/ai00021p.pdf

WITNESS LIST

PANEL ONE

Ms. Davi M. D'Agostino, Director
Defense Capabilities and Management
U.S. Government Accountability Office

Professor Allen Weinstein
Archivist of the United States
National Archives and Records Administration

Mr. J. William Leonard, Director
Information Security Oversight Office
National Archives and Records Administration

Mr. Robert Rogalski,
Acting Deputy Under Secretary of Defense
Counterintelligence and Security
Department of Defense

Mr. Glenn S. Podonsky, Director
Office of Security and Safety Performance Assurance
U.S. Department of Energy

PANEL TWO

Mr. Thomas Blanton,
Executive Director
National Security Archive
George Washington University

Dr. Anna Nelson
Distinguished Historian in Residence
American University

Mr. Matthew Aid
Washington, D.C.