Attachment 5

THE FREEDOM OF INFORMATION ACT

5 U.S.C. § 552

As Amended in 2002

§ 552. Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public--

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying--

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;

(C) administrative staff manuals and instructions to staff that affect a member of the public;

(D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and

(E) a general index of the records referred to under subparagraph (D);

unless the materials are promptly published and copies offered for sale. For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction, or copies of records referred to in subparagraph (D). However, in each case the justification for the deletion shall be explained fully in writing, and the extent of such deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of an index on request at a cost not to exceed the direct cost of duplication. Each agency shall make the index referred to in subparagraph (E) available by computer telecommunications by December 31, 1999. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if--

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(E) An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) shall not make any record available under this paragraph to--

(i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or

(ii) a representative of a government entity described in clause (i).

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that--

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii)

if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section--

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed $250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo, provided that the court's review of the matter shall be limited to the record before the agency.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial

weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court other wise directs for good cause is shown.

(D) Repealed by Pub. L. 98-620, Title IV, 402(2), Nov. 8, 1984, 98 Stat. 3335, 3357.

(E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--

(i) determine within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

(B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days, except as provided in clause (ii) of this subparagraph.

(ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C).

(iii) As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular requests--

(I) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

(III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.

(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(C)(i) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(ii) For purposes of this subparagraph, the term "exceptional circumstances" does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.

(iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing the request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.

(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.

(iii) This subparagraph shall not be considered to affect the requirement under subparagraph (C) to exercise due diligence.

(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records--

(I) in cases in which the person requesting the records demonstrates a compelling need; and

(II) in other cases determined by the agency.

(ii) Notwithstanding clause (i), regulations under this subparagraph must ensure--

(I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and

(II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.

(iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

(iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.

(v) For purposes of this subparagraph, the term "compelling need" means--

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

(vi) A demonstration of a compelling need by a person

making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person's knowledge and belief.

(F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.

(b) This section does not apply to matters that are--

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared

by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and--

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize the withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States a report which shall cover the preceding fiscal year and which shall include--

(A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(B)(i) the number of appeals made by persons under subsection (a)(6),

the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and

(ii) a complete list of all statutes that the agency relies upon to authorize the agency to withhold information under subsection (b)(3), a description of whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;

(C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median number of days that such requests had been pending before the agency as of that date;

(D) the number of requests for records received by the agency and the number of requests which the agency processed;

(E) the median number of days taken by the agency to process different types of requests;

(F) the total amount of fees collected by the agency for processing requests; and

(G) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests.

(2) Each agency shall make each such report available to the public including by computer telecommunications, or if computer telecommunications means have not been established by the agency, by other electronic means.

(3) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Government Reform and Oversight of the House of Representatives and the Chairman and ranking minority member of the Committees on Governmental Affairs and the Judiciary of the Senate, no later than April 1 of the year in which each such report is issued, that such reports are available by electronic means.

(4) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.

(5) The Attorney General of the United States shall submit an annual report on or before April 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4). Such report shall also include a description of the efforts undertaken by the Department of

Justice to encourage agency compliance with this section.

(f) For purposes of this section, the term--

(1) "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(2) "record" and any other term used in this section in reference to information includes any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.

(g) The head of each agency shall prepare and make publicly available upon request, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including--

(1) an index of all major information systems of the agency;

(2) a description of major information and record locator systems maintained by the agency; and

(3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

Go to: DOJ FOIA Page // Justice Department Home Page

Last Updated December 23, 2002
usdoj/jmd/ls/caf

Attachment 6

United States Government Accountability Office

GAO

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

March 2006

MANAGING SENSITIVE INFORMATION

Departments of Energy and Defense Policies and Oversight Could Be Improved

This Report Is Temporarily Restricted Pending Official Public Release.

G A O

Accountability * Integrity * Reliability

GAO-06-369

March 2006

GAO
Accountability·Integrity·Reliability

Highlights

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

MANAGING SENSITIVE INFORMATION

Departments of Energy and Defense Policies and Oversight Could Be Improved

Why GAO Did This Study

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

What GAO Recommends

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

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

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

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

What GAO Found

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

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

Contents

Letter 1

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

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

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

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

Table

Table 1: FOIA Exemptions 5

Figure

Figure 1: DOE's OUO Stamp 7

Abbreviations

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

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

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

March 7, 2006

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

Dear Mr. Chairman:

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

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

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

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

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

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

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

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

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

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

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

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

Results in Brief

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

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

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

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

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

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

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

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

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

Table 1: FOIA Exemptions

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

Sources: FOIA and GAO analysis.

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

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

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

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

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

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

Figure 1: DOE's OUO Stamp

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____

Department of Energy review required before public release

Name/Org: _____ **Date:** _____

Guidance (if applicable): _____

Source: DOE.

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

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

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

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

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

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

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

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

Neither DOE nor DOD Requires Training or Conducts Oversight

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

OUO and FOUO Training Is Generally Not Required

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

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

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

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

Oversight of OUO and FOUO Programs Is Lacking

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

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

Conclusions

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

Recommendations for Executive Action

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

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

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

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

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

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

Agency Comments and Our Evaluation

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

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

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

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

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

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

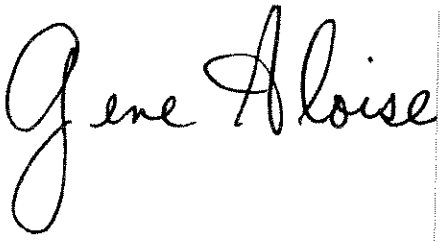
As agreed with your offices unless you publicly release the contents of this report earlier, we plan no further distribution until 30 days from its date. We will then send copies of this report to the Secretary of Energy; the Secretary of Defense; the Director, Office of Management and Budget; and interested congressional committees. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

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

Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Sincerely yours,

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



Gene Aloise
Director, Natural Resources and Environment

Appendix I: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

February 7, 2006

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

Dear Mr. Aloise:

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

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

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

Printed with soy ink on recycled paper

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

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

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

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

Sincerely,

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

Enclosures

Appendix

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

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

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

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

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

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

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

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

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

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

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

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

Appendix II: Comments from the Department of Defense

INTELLIGENCE

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

FEB 0 7 2006

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

Dear Ms. D'Agostino:

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

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

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

Sincerely,

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

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

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

DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS

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

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

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

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

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

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

(p. 14/GAO Draft Report)

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

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

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

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

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

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Acknowledgments

In addition to the contacts named above, Ann Borseth and Ned Woodward, Assistant Directors; Nancy Crothers; Doreen Feldman; Mattias Fenton; Adam Hatton; David Keefer; William Lanouette; Gregory Marchand; David Mayfield; James Reid; Marc Schwartz; Kevin Tarmann; Cheryl Weissman; and Jena Whitley made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Attachment 7

APPENDIX C

CONTROLLED UNCLASSIFIED INFORMATION

Section 1

Introduction

1-100 General

a. The requirements of the Information Security Program apply only to information that requires protection to prevent damage to the national security and has been classified in accordance with E.O. 12958 or its predecessors. There are other types of information that require application of controls and protective measures for a variety of reasons. This information is known as "unclassified controlled information." Since classified information and unclassified controlled information exist side-by-side in the work environments-often in the same documents-this appendix is provided as an attempt to avoid confusion and promote proper handling. It covers several types of unclassified controlled information, and provides basic information about the nature of this information and the procedures for identifying and controlling it. In some cases, the appendix refers to other DoD Directives that provide more detailed guidance.

b. The types of information covered in this appendix include "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DoD Unclassified Controlled Nuclear Information," "Sensitive Information" as defined in the Computer Security Act of 1987, and information contained in technical documents.

Section 2

For Official Use Only Information.

2-200 Description

a. "For Official Use Only (FOUO)" is a designation that is applied to *unclassified* information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions which may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

(1) Information which is currently and properly classified.
(2) Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
(3) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
(4) Information such as trade secrets and commercial or financial information obtained from a

company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.
(5) Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
(6) Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
(7) Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source, (e) disclose investigative techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.
(8) Certain records of agencies responsible for supervision of financial institutions.
(9) Geological and geophysical information concerning wells.

b. Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. "For Official Use Only" is applied to information that is exempt under one of the *other* eight categories. So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that (1) information cannot be classified and FOUO at the same time, and (2) information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

c. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories *and* there must be a legitimate Government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still qualify for withholding under the FOIA.

2-201 Markings

a. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

b. Unclassified documents and material containing FOUO information shall be marked as follows:

(1) Documents will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).
(2) Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.
(3) Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings which alert the holder or viewer that the material contains FOUO information.
(4) FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

This document contains information exempt from mandatory disclosure under the FOIA.

Exemption(s) _____ apply.

c. Classified documents and material containing FOUO information shall be marked as required by Chapter V of this regulation, with FOUO information identified as follows:

(1) Overall markings on the document shall follow the rules in Chapter 5. No special markings are required on the face of the document because it contains FOUO information.
(2) Portions of the document shall be marked with their classification as required by Chapter 5. If there are unclassified portions that contain FOUO information, they shall be marked with "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."
(3) Pages of the document that contain classified information shall be marked as required by Chapter 5. Pages that contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

d. Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

e. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text.

2-202 Access to FOUO Information

FOUO information may be disseminated within the DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary 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. (Special restrictions may apply to information covered by the Privacy Act.) 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.

2-203 Protection of FOUO Information

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO information shall be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked desks, file cabinets, bookcases, locked rooms, or similar items.

b. FOUO documents and material may be transmitted via first class mail, parcel post or-for bulk shipments-fourth class mail. Electronic transmission of FOUO information (voice, data or facsimile) should be by approved secure communications systems whenever practical.

c. Record copies of FOUO documents shall be disposed of in accordance with the Federal Records Act (44 U.S.C. 33) and Component records management directives. Non-record FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

2-204 Further Guidance

Further guidance on one type of FOUO information is contained in DoD 5400.11-R, Department of

Defense Privacy Program.

Section 3

Sensitive But Unclassified and Limited Official Use Information

3-300 Description

Sensitive But Unclassified (SBU) information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act. Before 26 May 1995, this information was designated and marked "Limited Official Use (LOU)." The LOU designation will no longer be used.

3-301 Markings

The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. When SBU information is included in DoD documents, they shall be marked as if the information were For Official Use Only. There is no requirement to remark existing material containing SBU information.

3-302 Access to SBU Information

Within the Department of Defense, the criteria for allowing access to SBU information are they same as those used for FOUO information.

3-303 Protection of SBU Information

Within the Department of Defense, SBU information shall be protected as required for FOUO information.

Section 4

Drug Enforcement Administration Sensitive Information

4-400 Description

DEA Sensitive information is unclassified information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The Administrator and certain other officials of the DEA have been authorized to designate information as DEA Sensitive; the Department of Defense has agreed to implement protective measures for DEA Sensitive information in its possession. Types of information to be protected include:

a. Information and material that is investigative in nature;
b. Information and material to which access is restricted by law;
c. Information and material that is critical to the operation and mission of the DEA; and
d. Information and material the disclosure of which would violate a privileged relationship.

4-401 Markings

a. Unclassified documents containing DEA Sensitive information shall be marked "DEA Sensitive" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

b. In unclassified documents, each page containing DEA Sensitive information shall be marked "DEA Sensitive" top and bottom. Classified documents containing DEA Sensitive information shall be marked as required by Chapter 5, except that pages containing DEA Sensitive information but no classified information will be marked "DEA Sensitive" top and bottom.

c. Portions of DoD documents that contain DEA Sensitive information shall be marked "(DEA)" at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA Sensitive information, the "DEA" marking shall be included along with the parenthetical classification marking.

4-402 Access to DEA Sensitive Information

Access to DEA Sensitive information shall be granted only to persons who have a valid need-to-know for the information. A security clearance is not required. DEA Sensitive information in the possession of the Department of Defense may not be released outside the Department without authorization by the DEA.

4-403 Protection of DEA Sensitive Information

a. DEA Sensitive material may be transmitted within CONUS by first class mail. Transmission outside CONUS must be by a means approved for transmission of Secret material. Non-government package delivery and courier services may not be used. The material shall be enclosed in two opaque envelopes or containers, the inner one marked "DEA Sensitive" on both sides. Electronic transmission of DEA Sensitive information within CONUS should be over secure communications circuits whenever possible; transmission outside CONUS must be over approved secure communications circuits.

b. Reproduction of DEA Sensitive information and material shall be limited to that required for operational needs.

c. DEA Sensitive material shall be destroyed by a means approved for destruction of Confidential material.

Section 5

DoD Unclassified Controlled Nuclear Information

5-500 Description

DoD Unclassified Controlled Nuclear Information (DoD UCNI) is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities. Information is Designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals to whom they have delegated the authority.

5-501 Markings

a. Unclassified documents and material containing DoD UCNI shall be marked as follows:

(1) The face of the document and the outside of the back cover (if there is one) shall be marked "DoD Unclassified Controlled Nuclear Information."
(2) Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion.

b. Classified documents and material containing DoD UCNI shall be marked in accordance with Chapter V, except that:

(1) Pages with no classified information but containing DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the top and bottom.
(2) Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion-in addition to the classification marking, where appropriate.

c. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains DoD UCNI.

d. Documents and material containing DoD UCNI and transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

DEPARTMENT OF DEFENSE

UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION

EXEMPT FROM MANDATORY DISCLOSURE

(5 U.S.C. 552(b)(3), as authorized by 10 U.S.C. 128)

e. Transmittal documents that have DoD UCNI attachments shall bear a statement: "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)."

5-502 Access to DoD UCNI

Access to DoD UCNI shall be granted only to persons who have a valid need-to-know for the information and are specifically eligible for access under the provisions of DoD Directive 5210.83, Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI).

5-503 Protection of DoD UCNI

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, DoD UCNI may be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked buildings, rooms, desks, file cabinets, bookcases, or similar items.

b. DoD UCNI may be transmitted by first class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DoD UCNI shall be over approved secure communications circuits.

c. Record copies of DoD UCNI documents shall be disposed of in accordance with the Federal Records

Act (44 U.S.C. 33) and Component records management directives. Non-record DoD UCNI documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

Section 6

Sensitive Information (Computer Security Act of 1987)

6-600 Description

a. The Computer Security Act of 1987 established requirements for protection of certain information in Federal Government automated information systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Act applies only to unclassified information that deserves protection. Second, unlike most other programs for protection of information, the Act is concerned with protecting the availability and integrity, as well as the confidentiality of information. Much of the information which fits the Act's definition of "sensitive" falls within the other categories of information discussed in this Appendix. Some does not.

6-601 Markings

There is no specific marking authorized for designation of "sensitive" information. If the information fits within one of the other categories of information described in this Appendix, the appropriate marking requirements apply.

6-602 Access to Sensitive Information

If sensitive information falls within one of the other categories of information described in this Appendix, the specific limitations on access for the appropriate category shall be applied. If it does not, access to the information shall be limited only to those with a valid need for such access in order to perform a legitimate organizational function, as dictated by common-sense principles of security management.

6-603 Protection of Sensitive Information

Information on DoD AIS systems that is determined to be "sensitive" within the meaning of the Computer Security Act of 1987 shall be provided protection that is:

a. Determined after thorough consideration of the value and sensitivity of the information and the probable adverse impact of loss of its availability, integrity or confidentiality;
b. In compliance with applicable DoD policy and requirements for security of information within automated systems;
c. Commensurate with the degree of protection required for the category of information described in this Appendix to which it belongs (if any); and
d. Based on sound application of risk management techniques and procedures.

6-604 Further Guidance

Further guidance is found in DoD Directive 5200.28, Security Requirements for Automated Data Processing (ADP) Systems, and related publications.

Section 7

Technical Documents

7-700 General

DoD Directive 5230.24 requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case-by-case exceptions to distribution limitations imposed by the statements.

7-701 Text of the Statements

Distribution Statement A

Approved for public release; distribution is unlimited.

Distribution Statement B

Distribution authorized to U.S. Government

agencies only; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement C

Distribution authorized to US Government agencies and their contractors; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement D

Distribution authorized to the DoD and US DoD contractors only; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement E

Distribution authorized to DoD Components only; [reason]; [date].

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement F

Further distribution only as directed by [controlling DoD office] or higher DoD authority; [date].

Distribution Statement X

Distribution authorized to US Government agencies and private individuals or enterprises eligible to obtain

export-controlled technical data in accordance with DoD Directive 5230.25; [date].

Controlling DoD office is [controlling DoD office].

Attachment 8

U.S. Reclassifies Many Documents in Secret Review

By SCOTT SHANE, The New York Times

WASHINGTON (Feb. 21) - In a seven-year-old secret program at the National Archives, intelligence agencies have been removing from public access thousands of historical documents that were available for years, including some already published by the State Department and others photocopied years ago by private historians.

National Archives officials say the program has revoked access to about 9,500 documents, more than 8,000 of them since President Bush took office.

The restoration of classified status to more than 55,000 previously declassified pages began in 1999, when the Central Intelligence Agency and five other agencies objected to what they saw as a hasty release of sensitive information after a 1995 declassification order signed by President Bill Clinton. It accelerated after the Bush administration took office and especially after the 2001 terrorist attacks, according to archives records.

But because the reclassification program is itself shrouded in secrecy - governed by a still-classified memorandum that prohibits the National Archives even from saying which agencies are involved - it continued virtually without outside notice until December. That was when an intelligence historian, Matthew M. Aid, noticed that dozens of documents he had copied years ago had been withdrawn from the archives' open shelves.

Mr. Aid was struck by what seemed to him the innocuous contents of the documents - mostly decades-old State Department reports from the Korean War and the early cold war. He found that eight reclassified documents had been previously published in the State Department's history series, "Foreign Relations of the United States."

"The stuff they pulled should never have been removed," he said. "Some of it is mundane, and some of it is outright ridiculous."

After Mr. Aid and other historians complained, the archives' Information Security Oversight Office, which oversees government classification, began an audit of the reclassification program, said J. William Leonard, director of the office.

Mr. Leonard said he ordered the audit after reviewing 16 withdrawn documents and concluding that none should be secret.

"If those sample records were removed because somebody thought they were classified, I'm shocked and disappointed," Mr. Leonard said in an interview. "It just boggles the mind."

If Mr. Leonard finds that documents are being wrongly reclassified, his office could

not unilaterally release them. But as the chief adviser to the White House on classification, he could urge a reversal or a revision of the reclassification program.

A group of historians, including representatives of the National Coalition for History and the Society of Historians of American Foreign Relations, wrote to Mr. Leonard on Friday to express concern about the reclassification program, which they believe has blocked access to some material at the presidential libraries as well as at the archives.

Among the 50 withdrawn documents that Mr. Aid found in his own files is a 1948 memorandum on a C.I.A. scheme to float balloons over countries behind the Iron Curtain and drop propaganda leaflets. It was reclassified in 2001 even though it had been published by the State Department in 1996.

Another historian, William Burr, found a dozen documents he had copied years ago whose reclassification he considers "silly," including a 1962 telegram from George F. Kennan, then ambassador to Yugoslavia, containing an English translation of a Belgrade newspaper article on China's nuclear weapons program.

Under existing guidelines, government documents are supposed to be declassified after 25 years unless there is particular reason to keep them secret. While some of the choices made by the security reviewers at the archives are baffling, others seem guided by an old bureaucratic reflex: to cover up embarrassments, even if they occurred a half-century ago.

One reclassified document in Mr. Aid's files, for instance, gives the C.I.A.'s assessment on Oct. 12, 1950, that Chinese intervention in the Korean War was "not probable in 1950." Just two weeks later, on Oct. 27, some 300,000 Chinese troops crossed into Korea.

Mr. Aid said he believed that because of the reclassification program, some of the contents of his 22 file cabinets might technically place him in violation of the Espionage Act, a circumstance that could be shared by scores of other historians. But no effort has been made to retrieve copies of reclassified documents, and it is not clear how they all could even be located.

"It doesn't make sense to create a category of documents that are classified but that everyone already has," said Meredith Fuchs, general counsel of the National Security Archive, a research group at George Washington University. "These documents were on open shelves for years."

The group plans to post Mr. Aid's reclassified documents and his account of the secret program on its Web site, www.gwu.edu/~nsarchiv, on Tuesday.

The program's critics do not question the notion that wrongly declassified material should be withdrawn. Mr. Aid said he had been dismayed to see "scary" documents in open files at the National Archives, including detailed instructions on the use of high explosives.

But the historians say the program is removing material that can do no conceivable harm to national security. They say it is part of a marked trend toward greater secrecy under the Bush administration, which has increased the pace of classifying documents, slowed declassification and discouraged the release of some material under the Freedom of Information Act.

Experts on government secrecy believe the C.I.A. and other spy agencies, not the White House, are the driving force behind the reclassification program.

"I think it's driven by the individual agencies, which have bureaucratic sensitivities to protect," said Steven Aftergood of the Federation of American Scientists, editor of the online weekly Secrecy News. "But it was clearly encouraged by the administration's overall embrace of secrecy."

National Archives officials said the program had revoked access to 9,500 documents, more than 8,000 of them since President Bush took office. About 30 reviewers - employees and contractors of the intelligence and defense agencies - are at work each weekday at the archives complex in College Park, Md., the officials said.

Archives officials could not provide a cost for the program but said it was certainly in the millions of dollars, including more than $1 million to build and equip a secure room where the reviewers work.

Michael J. Kurtz, assistant archivist for record services, said the National Archives sought to expand public access to documents whenever possible but had no power over the reclassifications. "The decisions agencies make are those agencies' decisions," Mr. Kurtz said.

Though the National Archives are not allowed to reveal which agencies are involved in the reclassification, one archivist said on condition of anonymity that the C.I.A. and the Defense Intelligence Agency were major participants.

A spokesman for the C.I.A., Paul Gimigliano, said that the agency had released 26 million pages of documents to the National Archives since 1998 and that it was "committed to the highest quality process" for deciding what should be secret.

"Though the process typically works well, there will always be the anomaly, given the tremendous amount of material and multiple players involved," Mr. Gimigliano said.

A spokesman for the Defense Intelligence Agency said he was unable to comment on whether his agency was involved in the program.

Anna K. Nelson, a foreign policy historian at American University, said she and other researchers had been puzzled in recent years by the number of documents pulled from the archives with little explanation.

"I think this is a travesty," said Dr. Nelson, who said she believed that some reclassified material was in her files. "I think the public is being deprived of what history is really about: facts."

The document removals have not been reported to the Information Security Oversight Office, as the law has required for formal reclassifications since 2003.

The explanation, said Mr. Leonard, the head of the office, is a bureaucratic quirk. The intelligence agencies take the position that the reclassified documents were never properly declassified, even though they were reviewed, stamped "declassified," freely given to researchers and even published, he said.

Thus, the agencies argue, the documents remain classified — and pulling them from public access is not really reclassification.

Mr. Leonard said he believed that while that logic might seem strained, the agencies were technically correct. But he said the complaints about the secret program, which prompted his decision to conduct an audit, showed that the government's system for deciding what should be secret is deeply flawed.

"This is not a very efficient way of doing business," Mr. Leonard said. "There's got to be a better way."

Attachment 9

THE WHITE HOUSE
WASHINGTON

March 19, 2002

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM:

ANDREW H. CARD, JR.
Assistant to the President and Chief of Staff

SUBJECT:

Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security

As noted in many discussions during the past several months, you and your department or agency have an obligation to safeguard Government records regarding weapons of mass destruction. Weapons of mass destruction include chemical, biological, radiological, and nuclear weapons. Government information, regardless of its age, that could reasonably be expected to assist in the development or use of weapons of mass destruction, including information about the current locations of stockpiles of nuclear materials that could be exploited for use in such weapons, should not be disclosed inappropriately.

I asked the Acting Director of the Information Security Oversight Office and the Co-Directors of the Justice Department's Office of Information and Privacy to prepare guidance for reviewing Government information in your department or agency regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our Nation and the safety of our people. Their guidance is attached, and it should be distributed to appropriate officials within your department or agency, together with this memorandum, to assist in your undertaking an immediate reexamination of current measures for identifying and safeguarding all such information at your department or agency.

All departments and agencies should review their records management procedures and, where appropriate, their holdings of documents to ensure that they are acting in accordance with the attached guidance. They should report the completion, or status, of their review to my office through the Office of Homeland Security no later than 90 days from the date of this memorandum.

If agency officials need assistance in determining the classification status of records related to the development or use of weapons of mass destruction, they should contact the Information Security Oversight Office, at 202-219-5250. For assistance in determining the classification of nuclear and radiological weapons classified under the Atomic Energy Act,

they should contact the Department of Energy's Office of Security, at 202-586-3345. If they need assistance in applying exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified information, they should contact the Justice Department's Office of Information and Privacy (OIP), at 202-514-3642, or consult OIP's FOIA Web site at www.usdoj.gov/04foia/index/html [sic].

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408

March 19, 2002

MEMORANDUM FOR DEPARTMENTS AND AGENCIES

FROM:

LAURA L.S. KIMBERLY
Acting Director
Information Security Oversight Office

RICHARD L. HUFF
DANIEL J. METCALFE
Co-Directors
Office of Information and Privacy
Department of Justice

SUBJECT:

Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security

At the request of the Assistant to the President and Chief of Staff, we have prepared this memorandum to provide guidance for reviewing Government information regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation or threaten public safety. It is appropriate that all federal departments and agencies consider the need to safeguard such information on an ongoing basis and also upon receipt of any request for records containing such information that is made under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). Consistent with existing law and policy, the appropriate steps for safeguarding such information will vary according to the sensitivity of the information involved and whether the information currently is classified.

I. Classified Information

- If the information currently is classified and is equal to or less than 25 years old, it should remain classified in accordance with Executive Order 12958, Sec. 1.5 and Sec. 1.6. Although classified information generally must be declassified within 10 years of

its original classification, classification or reclassification may be extended for up to 25 years in the case of information that could reasonably be expected to "reveal information that would assist in the development or use of weapons of mass destruction." Id., Sec. 1.6(d)(2).

- If the information is more than 25 years old and is still classified, it should remain classified in accordance with Executive Order 12958, Sec. 3.4(b)(2), which authorizes agency heads to exempt from automatic declassification any "specific information, the release of which should be expected to ... reveal information that would assist in the development or use of weapons of mass destruction." (Agencies should note that the automatic declassification date for any classified information over 25 years old that involves the equities of more than one agency was extended under April 2003 by Executive Order 13142. Agencies have until then to exempt such information from automatic declassification under any one of the pertinent exemption categories in Executive Order 12958, Sec. 3.4(b).)

  In this regard, agencies should note that Department of Defense (DOD) information that involves the equities of more than one DOD component is considered to have multi-agency equities. Information maintained by the Defense Technical Information Center (DTIC) or the National Archives and Records Administration (NARA) also is deemed to have multi-agency equities, i.e., those pertaining to DTIC or NARA and those pertaining to the component agency or agencies that created the information.

II. Previously Unclassified or Declassified Information

- If the information, regardless of age, never was classified and never was disclosed to the public under proper authority, but it could reasonably be expected to assist in the development or use of weapons of mass destruction, it should be classified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8 (d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).

- If such sensitive information, regardless of age, was classified and subsequently was declassified, but it never was disclosed to the public under proper authority, it should be reclassified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8(d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).

III. Sensitive But Unclassified Information

In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.

All departments and agencies should ensure that in taking necessary and appropriate actions

to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions. See *FOIA Post*, "New Attorney General FOIA Memorandum Issued" (posted 10/15/01) (found at www.usdoj.gov/oip/foiapost/2001foiapost19.htm), which discusses and provides electronic links to further guidance on the authority available under Exemption 2 of the FOIA, 5 U.S.C. § 552 (b)(2), for the protection of sensitive critical infrastructure information. In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552 (b)(4).

As the accompanying memorandum from the Assistant to the President and Chief of Staff indicates, federal departments and agencies should not hesitate to consult with the Office of Information and Privacy, either with general anticipatory questions or on a case-by-case basis as particular matters arise, regarding any FOIA-related homeland security issue. Likewise, they should consult with the Information Security Oversight Office on any matter pertaining to the classification, declassification, or reclassification of information regarding the development or use of weapons of mass destruction, or with the Department of Energy's Office of Security if the information concerns nuclear or radiological weapons.

HTML from hardcopy original by FAS

Justice Department version: http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm

Attachment 10

NATIONAL

Government withholds 'sensitive-but-unclassified' information

By LANCE GAY
Scripps Howard News Service
February 02, 2006

WASHINGTON - Connecticut Attorney General Richard Blumenthal calls them "secrecy orders" - nondisclosure agreements that the federal government is requiring citizens in his state to sign before they can see plans for a liquefied-natural-gas station on scenic Long Island Sound.

The restrictions are just another example of government efforts to restrict widespread public release of so-called sensitive-but-unclassified information.

Government agencies have withdrawn from public scrutiny thousands of pages of information - ranging from information on the location of nuclear plants, to plant diseases that could devastate crops, to designs of bridge abutments.

The information clampdown is in force in varying degrees at all of the federal agencies. After the Department of Labor's Occupational Health and Safety Administration investigated high injury rates among workers at the Portland, Ore., airport, the Transportation Security Administration (TSA) in 2004 blocked any public release of OSHA's findings on the grounds it contained sensitive-but-unclassified information.

Environmental groups and other activists complain that routine data on the dangers of nuclear plants and chemical-plant emissions now have dried up.

And information is not just being withheld from the public. The TSA also has refused to give local governments information on rail shipments of hazardous materials going through their communities on the grounds that it is sensitive but unclassified and can't be shared.

In the case of the liquefied-natural-gas station, the restrictions represent a compromise between the need to keep sensitive information out of the hands of terrorists and the rights of citizens to obtain public information on safety and environmental issues, said Tamara Young-Allen, spokeswoman for the Federal Energy Commission.

"We think it works very well," Young-Allen said, noting that her agency helps decide the locations of natural-gas pipelines, among other issues. "Would you want a map of those pipeline connects so a terrorist sitting in a cave in Afghanistan could get that information?"

But the Federal Energy Commission's procedures differ widely from other federal agencies - and that seems to be a problem.

President Bush says the federal government needs a unified approach to dealing with sensitive-but-unclassified information, and among the first orders he's given new Director of

National Security John Negroponte is to come up with one. Bush said he wants final recommendations for any changes by December.

The movement to declare some government information as sensitive but unclassified has been one of the most contentious issues the government has undertaken since the 9/11 attacks.

The TSA appears to be the most aggressive in enforcing the requirements. After declaring no-fly areas around nuclear power plants, the TSA ordered the Airline Owners and Pilots Association to take down from its Web site maps informing pilots where these areas were. The TSA in 2004 also asked news organizations to remove references to security problems at the Rochester, N.Y., airport that were exposed by a contractor in testimony before a congressional committee.

Steven Aftergood, an analyst with the Federation of American Scientists who publishes the newsletter Secrecy News, said the effort has created turmoil in the government, as federal bureaucrats have tried to figure out what is sensitive-but-unclassified information and how to segregate it from the information they regularly release.

"The government's information policy is a state of near-chaos," Aftergood said, noting there's no consistency for dealing with sensitive-but-unclassified information - not only with the public, but with federal contractors, and even among government agencies.

Aftergood said the basic problem the government faces is that there is no agreement on what constitutes "sensitive-but-unclassified." He said he doubts it is possible to write a uniform definition.

A 2004 study by the Congressional Research Service found that agencies are creating their own definitions based on interpretations of patent and privacy laws, Cold War restrictions on sales of technology to communist countries, and even a 2002 letter from then-Attorney General John Ashcroft directing federal agencies to take the broadest possible exemptions to prevent release of documents under the Freedom of Information Act.

Aftergood also questioned why Negroponte is being assigned to spearhead the review of policies, when his job is to oversee and coordinate classified programs. Sensitive-but-unclassified information doesn't involve classified information, he noted.

Negroponte spokesman Carl Kropf responded by saying that part of Negroponte's job involves coordinating more efficient ways of sharing intelligence across the government.

Kropf said the current approach to handling the material has resulted in confusion. "There is some concern that the existence of multiple secret-but-unclassified designations - each governed by its own unique set of procedures - adds a layer of complexity to efforts to share information," he said.

It's too early to say what changes will be made, or if they will result in more information being withheld by the government.

"The goal of the effort is to enhance the sharing of information amongst those entities responsible for protecting our communities from future attack," Kropf said.

(Contact Lance Gay at GayL(at)SHNS.com.)

Attachment 11

the White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
December 16, 2005

Memorandum for the Heads of Executive Departments and Agencies

SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment

Ensuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector entities, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror. Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108 458) (IRTPA), my Administration is working to create an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information (as defined in Executive Order 13388 of October 25, 2005).

Section 1016 of IRTPA supplements section 892 of the Homeland Security Act of 2002 (Public Law 107 296), Executive Order 13311 of July 29, 2003, and other Presidential guidance, which address various aspects of information access. On April 15, 2005, consistent with section 1016(f) of IRTPA, I designated the program manager (PM) responsible for information sharing across the Federal Government. On June 2, 2005, my memorandum entitled "Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment" directed that the PM and his office be part of the Office of the Director of National Intelligence (DNI), and that the DNI exercise authority, direction, and control over the PM and ensure that the PM carries out his responsibilities under IRTPA. On October 25, 2005, I issued Executive Order 13388 to facilitate the work of the PM and the expeditious establishment of the ISE and restructure the Information Sharing Council (ISC), which provides advice concerning and assists in the establishment, implementation, and maintenance of the ISE.

On June 2, 2005, I also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in section D of Homeland Security Presidential Directive 1 and other relevant presidential guidance with respect to information sharing. The ISPCC is the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM, and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses.

Section 1016(d) of IRTPA calls for leveraging all ongoing efforts consistent with establishing the ISE, the issuance of guidelines for acquiring, accessing, sharing, and using information in support of the ISE and for protecting privacy and civil liberties in the development of the ISE, and the promotion of a culture of information sharing. Consistent with the Constitution and the laws of the United States, including section 103 of the National Security Act of 1947, as amended, and sections 1016 and 1018 of IRTPA, I hereby direct as follows:

1. Leveraging Ongoing Information Sharing Efforts in the Development of the ISE. The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.

a. The DNI shall direct the PM to conduct and complete, within 90 days after the date of this memorandum, in consultation with the ISC, a comprehensive evaluation of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies. Such evaluation shall assess such resources for their utility and integrative potential in furtherance of the establishment of the ISE and shall identify any unnecessary redundancies.

b. To ensure that the ISE supports the needs of executive departments and agencies with counterterrorism responsibilities, and consistent with section 1021 of IRTPA, the DNI shall direct the PM, jointly with the Director of the National Counterterrorism Center (NCTC), and in coordination with the heads of relevant executive departments and agencies, to review and identify the respective missions, roles, and responsibilities of such executive departments and agencies, both as producers and users of terrorism information, relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information. The findings shall be reviewed through the interagency policy coordination process, and any recommendations for the further definition, reconciliation, or alteration of such missions, roles, and responsibilities shall be submitted, within 180 days after the date of this memorandum, by the DNI to the President for approval through the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT) and the Assistant to the President for National Security Affairs (APNSA). This effort shall be coordinated as appropriate with the tasks assigned under the Guidelines set forth in section 2 of this memorandum.

c. Upon the submission of findings as directed in the preceding paragraph (1(b)), the DNI shall direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies. These policies, procedures, and architectures shall be reviewed through the interagency policy coordination process, and shall be submitted, within 180 days after the submission of findings as directed in the preceding paragraph (1(b)), by the DNI to the President for approval through the APHS-CT and the APNSA.

2. Information Sharing Guidelines. Consistent with section 1016(d) of IRTPA, I hereby issue the following guidelines and related requirements, the implementation of which shall be conducted in consultation with, and with support from, the PM as directed by the DNI:

a. Guideline 1 - Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE

The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.

Consistent with Executive Order 13388 and IRTPA, the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security, and the Attorney General, shall develop and issue, within 90 days after the date of this memorandum, common standards (i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use or disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that include the appropriate method for the Government-wide adoption and implementation of such standards. Such standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector. Within 90 days after the issuance of such standards, the Secretary of Homeland Security and the Attorney General shall jointly disseminate such standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not. The DNI may amend the common standards from time to time as appropriate through the same process by which the DNI issued them.

b. Guideline 2 - Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws and executive orders and directives, the protection of national security, and the protection of the information privacy rights and other legal rights of Americans.

Within 180 days after the date of this memorandum, the Secretary of Homeland Security and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI, and consistent with the findings of the counterterrorism missions, roles, and responsibilities review under section 1 of this memorandum, shall:

(i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and

(ii) submit to the President for approval, through the APHS-CT and the APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

c. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information

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 (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders 13311 and 13388, section 892 of the Homeland Security Act of 2002, section 1016 of IRTPA, section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

(i) Within 90 days after the date of this memorandum, each executive department and agency will conduct an inventory of its SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of its existing SBU procedures. The results of each inventory shall be reported to the DNI, who shall provide the compiled results to the Secretary of Homeland Security and the Attorney General.

(ii) Within 90 days after receiving the compiled results of the inventories required under the preceding paragraph (i), the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, shall submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information in the manner described in paragraph (iv) below.

(iii) Within 1 year after the date of this memorandum, the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, shall submit to the President for approval recommendations for the standardization of SBU procedures for all types of information not addressed by the preceding paragraph (ii) in the manner described in paragraph (iv) below.

(iv) All recommendations required to be submitted to the President under this Guideline shall be submitted through the Director of the Office of Management and Budget (OMB), the APHS-CT, and the APNSA, as a report that contains the following:

(A) recommendations for government-wide policies and procedures to standardize SBU procedures;

(B) recommendations, as appropriate, for legislative, policy, regulatory, and administrative changes; and

(C) an assessment by each department and agency participating in the SBU procedures review process of the costs and budgetary considerations for all proposed changes to marking conventions, handling caveats, and other procedures pertaining to SBU information.

(v) Upon the approval by the President of the recommendations submitted under this Guideline, heads of executive departments and agencies shall ensure on an ongoing basis that such recommendations are fully implemented in such department or agency, as applicable. The DNI shall direct the PM to support executive departments and agencies in such implementation, as well as in the development of relevant guidance and training programs for the standardized SBU procedures.

d. Guideline 4 - Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies. To that end, policies and procedures to facilitate such informational access and exchange, including those relating to the handling of information received from foreign governments, must be established consistent with applicable laws and executive orders and directives.

Within 180 days after the date of this memorandum, the Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall review existing authorities and submit to the President for approval, through the APHS-CT and the APNSA, recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

e. Guideline 5 - Protect the Information Privacy Rights and Other Legal Rights of Americans

As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.

(i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.

(ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

3. Promoting a Culture of Information Sharing. Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.

Accordingly, each head of an executive department or agency that possesses or uses intelligence or terrorism information shall:

a. within 90 days after the date of this memorandum, designate a senior official who possesses knowledge of the operational and policy aspects of information sharing to (i) provide accountability and oversight for terrorism information sharing within such department and agency, (ii) work with the PM, in consultation with the ISC, to develop high level information sharing performance measures for the department or agency to be assessed no less than semiannually, and (iii) provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing;

b. within 180 days after the date of this memorandum, develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information. Such guidelines and training shall seek to reduce obstructions to sharing, consistent with applicable laws and regulations. Accountability efforts shall include the requirement to add a performance evaluation element on information sharing to employees' annual Performance Appraisal Review, as appropriate, and shall focus on the sharing of information that supports the mission of the recipient of the information; and

c. bring to the attention of the Attorney General and the DNI, on an ongoing basis, any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information and that such department or agency head believes is not required by applicable laws or to protect the information privacy rights and other legal rights of Americans. The Attorney General and the DNI shall review such restriction and jointly submit any recommendations for changes to such restriction to the APHS-CT and the APNSA for further review.

4. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide assistance and information to the DNI and the PM in the implementation of this memorandum.

5. This memorandum:

a. shall be implemented in a manner consistent with applicable laws, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

b. shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

c. shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

d. is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

GEORGE W. BUSH

###

Source: The White House