PSEUDO-SECRETS:

A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information

March 2006

The National Security Archive
www.nsarchive.org

The George Washington University
Gelman Library, Suite 701
2130 H Street, NW
Washington, D.C. 20037
Phone: 202/994-7000
Fax: 202/994-7005
nsarchiv@gwu.edu

CONTENTS

EXECUTIVE SUMMARY i

INTRODUCTION 1

METHODOLOGY 3

Impact of Card Memorandum 3
Policies on Protection of Sensitive Unclassified Information 4
What is Sensitive Unclassified Information? 4
Notes on Findings 5

FINDINGS 6

CARD MEMORANDUM AND PROTECTION OF UNCLASSIFIED HOMELAND SECURITY INFORMATION 6
Review of Records for WMD or Other Sensitive Information 6
Web Site Information Removal 6
Increased Emphasis on Using Applicable FOIA Exemptions 7
Implementing New Security and Safeguarding Measures 7
Dissemination of Card Memorandum 7
No Records or No Response 7

AGENCY CONTROL OF SENSITIVE UNCLASSIFIED INFORMATION (SUI). 9
Authority for Policy 9
Definition and Guidance 12
Designation Authority 14
Decontrol Authority 16
Government Employees' Access to Protected Information 17
Physical Safeguards for Sensitive Information 19
Limitations on Use of Information Controls 20
Unclassified Information Policies and the Freedom of Information Act 21

AGENCY PROCESSING OF FOIA REQUESTS. 23
Processing Time 23
Disparity in Response 23

RECOMMENDATIONS 25
Monitoring of Protected Documents 25
A Black Hole 26
The Hidden Costs 26
A Unified System 26

FURTHER READING 30

APPENDIX I: Card Memorandum FOIA Requests, Summary of Agency Processing

APPENDIX II: Impact of Card Memorandum, By Agency

APPENDIX III: Sensitive Unclassified Information FOIA Requests, Summary of Agency Processing

APPENDIX IV: Sensitive Unclassified Information, Policies by Agency

APPENDIX V: Sensitive Unclassified Information, Distinct Policies

APPENDIX VI: Glossary of Acronyms

EXECUTIVE SUMMARY

Although the numerous investigations into the September 11 attacks on the United States each concluded that excessive secrecy interfered with the detection and prevention of the attacks, new secrecy measures have nonetheless proliferated. This is the first comprehensive Report to summarize the policies for protection of sensitive unclassified information from a wide range of federal agencies and departments and identify the significant security, budgetary, and government accountability risks attendant to unregulated and unmonitored secrecy programs.

The picture that emerges from the diverse policies examined shows little likelihood that Congress or the public will be able to assess whether these policies are being used effectively to safeguard the security of the American public, or abused for administrative convenience or for improper secrecy. Unlike classified records or ordinary agency records subject to FOIA, there is **no monitoring of or reporting on the use or impact of protective sensitive unclassified information markings. Nor is there a procedure for the public to challenge protective markings.** Given the wide variation of practices and procedures as well as some of their features, it is probable that these policies interfere with interagency information sharing, increase the cost of information security, and limit public access to vital information.

The September 11 attacks on the United States and a March 2002 directive from White House Chief of Staff Andrew H. Card to federal agencies, requesting a review of all records and policies concerning the protection of "sensitive but unclassified" information spurred Congress and agencies to increase controls on information. What followed was the significant removal of information from public Web sites, increased emphasis on FOIA exemptions for withholding, and the proliferation of new categories of information protection markings.

Using targeted FOIA requests and research, the Archive gathered data on the information protection policies of 37 **major agencies and components**. Of the agencies and components analyzed, **only 8 of 37 (or 22%) have policies that are authorized by *statute or regulation*** while the majority (24 out of 37, or 65%) follow information protection policies that were generated internally, for example by directive or other informal guidance. Eleven agencies reported no policy regarding sensitive unclassified information or provided no documents responsive to the Archive's request.

Among the agencies and components that together handle the vast majority of FOIA requests in the federal government, **28 distinct policies for protection of sensitive unclassified information** exist: some policies conflate information safeguarding markings with FOIA exemptions and some include definitions for protected information ranging from very broad or vague to extremely focused or limited.

- **8 out of the 28 policies (or 29%) permit *any employee* in the agency to designate sensitive unclassified information for protection**, including the Department of Homeland Security (DHS is now the largest agency in the federal government other than Defense, with more than 180,000 employees); 10 of the policies (or 35%) allow only senior or supervisory officials to mark information for protection; 7 policies (or 25%) allow departments or offices to name a particular individual to oversee information protection under the policy; and 3 policies (or 11%) do not clearly specify who may implement the policy.

- In contrast, **12 of the policies (or 43%) are unclear or do not specify how, and by whom, protective markings can be removed**. Only one policy includes a provision for automatic decontrolling after the passage of a period of time or particular event. This is in marked contrast to the classification* system, which provides for declassification after specified periods of time or the occurrence of specific events.

- **Only 7 out of 28 policies (or 25%) include qualifiers or cautionary restrictions that prohibit the use of the policy markings for improper purposes**, including to conceal embarrassing or illegal agency actions, inefficiency, or

* The term "classified" or "classification" refers to information designated as protected under Executive Order 12958, as amended by E.O. 13292.

administrative action. Again, this is distinguishable from the classification system, which explicitly prohibits classification for improper purposes.

- **There is no consistency among agencies as to how they treat protected sensitive unclassified information in the context of FOIA.** In a number of the agency policies, FOIA is specifically incorporated–either as a definition of information that may be protected or as a means to establish mandatory withholding of particular information subject to a sensitive unclassified information policy. Some agencies mandate ordinary review of documents before release, without regard to any protective marking. Others place supplemental hurdles that must be surmounted before sensitive information may be released to the public, for example the requirement of specific, case-by-case review by high-level officials for each document requested.

This Study finds that the procedures and regulations for safeguarding sensitive but unclassified information that were in use before September 11–particularly those protecting nuclear and other major, potentially-susceptible infrastructure information–differ markedly from the post-September 11 regulations. **The newest information protection designations are vague, open-ended, or broadly applicable,** thus raising concerns about the impact of such designations on access to information, free speech, and citizen participation in governance. As these findings suggest, more information control does not necessarily mean better information control. The implications certainly suggest that the time is ripe for a government-wide reform–with public input–of information safeguarding.

WHAT THE EXPERTS ARE SAYING

"[N]ever before have we had such a clear and demonstrable need for a seamless process for sharing and protecting information, regardless of classification."
-- J. William Leonard, ISOO Director (2003)[i]

"One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents."
-- Report, U.S. House of Representatives, Committee on Gov't Operations (1973)[ii]

"[T]hese designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."
-- Moynihan Commission Report (1997)[iii]

"[T]hose making SSI designation . . . should have special training, much as FOIA officers do, because they are being asked to make difficult balancing decisions among competing values."
-- Coalition of Journalists for Open Government (2004)[iv]

"Legally ambiguous markings, like sensitive but unclassified, sensitive homeland security information and for official use only, create new bureaucratic barriers to information sharing. These pseudo-classifications can have persistent and pernicious practical effects on the flow of threat information."
– Representative Christopher Shays (2005)[v]

"Terms such as 'SHSI' and 'SBU' describe broad types of potentially sensitive information that might not even fall within any of the FOIA exemptions."
-- Department of Justice, Freedom of Information Act Guide (2004)[vi]

"The fact that for official use only (FOUO) and other sensitive unclassified information (e.g. CONOPS, OPLANS, SOP) continues to be found on public web sites indicates that too often data posted are insufficiently reviewed for sensitivity and/or inadequately protected."
-- Sec. of Defense Donald Rumsfeld (2003)[vii]

"[V]ery little of the attention to detail that attends the security classification program is to be found in other information control marking activities."
– Harold C. Relyea,
Congressional Research Service (2005)[viii]

INTRODUCTION

Four months after the September 11 attacks, the *New York Times* published a front page story that reported "the government is still making available to the public hundreds of formerly secret documents that tell how to turn dangerous germs into deadly weapons."[1] That story started a chain of events including, in March 2002, explicit direction from President Bush's Chief of Staff Andrew H. Card for all federal agencies and departments to review their methods for safeguarding records regarding weapons of mass destruction (WMD), including chemical, biological, radiological, and nuclear weapons ("Card Memorandum"). Attached to the Card Memorandum was a memorandum from the Acting Director of the Information Security Oversight Office (ISOO) and the Co-Directors of the Justice Department's Office of Information and Privacy (OIP) ("ISOO-DOJ Guidance") that concerned handling classified, declassified, and sensitive but unclassified information.

Since that time there have been reports about the proliferation of new categories of "safeguarded" sensitive unclassified information, congressional and public criticism about unregulated "pseudo-classification," and calls for reform.[2] Aside from a few studies looking at the origins of protection of sensitive, unclassified information, however, there is very little information in the public domain that could be used to assess such safeguarding. This Study examines the implementation of the Card Memorandum, the attributes of the new safeguard markings, and the impact that this extra protection of sensitive unclassified information may have on information disclosure.

DOCUMENT CONTROL LABELS USED BY EXECUTIVE DEPARTMENTS AND AGENCIES

Control label:	[Number of agencies using it]
ACDA use only	1
Addressee only	1
Administrative-Internal use only	1
Administratively confidential	1
Administratively restricted	4
ATOMAL	2
ATOMAL/COSMIC	2
Company confidential	1
Confidential	1
Confidential-Administrative	1
Confidential FR	1
Confidential-Personnel	1
Continued control	1
Critical nuclear weapon design information	1
CRYPTO	1
Distribution to U.S. Government agencies only	1
Distribution restricted—See DoD map or Chart Catalog for Guidance or Release Outside the U.S. Government	1
Exdis	2
Eyes only	2
For (name) only	1
For official use only	11
For staff use only	1
Formerly restricted data	4
10S channel-eyes only	1
Information for official use only	1
Internal NASA use only	1
Internal office	1
Limdis	2
Limit distribution	1
Limited access	1
Limited access to	1
Limited distribution	1
Limited—For official use only	1
Limited information	1
Limited official use	9
NASA sensitive data	1
NATO	1
No distribution outside department	1
Nodis	2
Noforn	4
Nonpublic	1
Not public information	1
Official use only	8
Personal	1
Private	1
Privileged business information	1
Proprietary	1
Restricted	2
Restricted data	5
SIOP	1
SIOP-ESI	1
SIOP/Special handling required not releasable to foreign nationals	1
SPECAT	1
Sensitive	1
Sensitive-In confidence	1
Special handling required not releasable to foreign nationals	1
U.S. Government use only	1
Weapon data	1

List of 63 labels identified by the Foreign Operations and Government Information Subcommittee in 1972.

The government's safeguarding or restricting access to documents and other information that *does not fall* within the purview of the national security classification system has been an issue for decades. In its first omnibus hearings on the implementation of the Freedom of Information Act (FOIA), in 1972, the Foreign Operations and Government Information Subcommittee of the House Government Operations Committee raised the issue of the "secrecy terms" that are used to identify and restrict access to government information outside of the classification system. The subcommittee identified 63 separate terms at that time which, according to Chairman William Moorhead, "range[d] from the asinine to the absurd."[3]

> *I do not see how nine categories of information can be expanded to 63 secrecy stamps. It might require further legislation to convince the secrecy-minded bureaucrats that Congress meant what it said 5 years ago when it passed the first Freedom of Information Act.*
>
> *–Chairman William Moorhead, House Subcommittee on Foreign Operations and Gov't Operations (1973)*[ix]

The predominant congressional concern at that time was the overuse of control markings and distribution restrictions, applied to both classified and unclassified information, in the context of FOIA exemption 1, which permits information to be withheld because it is properly classified pursuant to Executive Order. In addition, the subcommittee evaluated

the implications of the new Executive Order and the attendant security of classified information: "It is a concern because the more stamps you put on documents the less security you are going to have at the very sensitive levels where maximum security should be always safeguarded."[4]

Following these early congressional discussions, little action was taken beyond the threatening message that Chairman Moorhead sent to federal agencies about their use of control markings. Nonetheless, it appears that the use of such markings decreased, and public discussion of the matter quieted down in the subsequent years. In 1977, President Jimmy Carter issued a Directive mandating federal protection of telecommunications materials "that could be useful to an adversary."[5] Subsequently, one of President Ronald Reagan's National Security Decision Directives referred to "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest" and, without further defining such information, ordered that it should be "protected in proportion to the threat of exploitation and the associated potential damage to the national security."[6]

The Computer Security Act of 1987 was passed in response to the proliferation of electronic communications and information systems and uncertainty about the nature of their security vulnerabilities. The Act defined "sensitive" information 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 . . . 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."[7] The implementation of the Computer Security Act, directed in part by guidance from the National Institute of Standards and Technology, emphasized a "risk-based approach" to safeguarding information, in which agencies in their discretion were to determine the required level of protection for designated "sensitive" information in their computer systems, based on the nature of the information.

In 1997, Senator Daniel Patrick Moynihan's Commission on Protecting and Reducing Government Secrecy recognized the mounting difficulties with the use by more than 40 departments and agencies of various protective markings for unclassified information: "there is little oversight of which information is designated as sensitive, and virtually any agency employee can decide which information is to be so regulated." As to the general lack of understanding and consistency in the management of such protected information, the Commission found: "these designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."[8]

Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.

– President Dwight D. Eisenhower[x]

Since the September 11 attacks and the inception of the War on Terrorism, new protective markings for unclassified information have been created, while numerous others have been updated, broadened, or used with increasing frequency. The Homeland Security Act of 2002 mandated information sharing among federal, state, and local authorities, and in conjunction directed the President to "identify and safeguard homeland security information that is sensitive but unclassified."[9] In 2003, President Bush delegated responsibility for protecting Sensitive Homeland Security Information (SHSI) to the Secretary of Homeland Security, but no regulations or other formalized SHSI protections have been implemented.

In December 2005, President Bush issued a memorandum for department heads regarding "Guidelines and Requirements in Support of the Information Sharing Environment." In this memo, the White House directed the agencies to develop standard procedures for handling Sensitive But Unclassified (SBU) information, including SHSI. These procedures, the memo asserted, "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." The memo prescribes several action items, beginning with mandatory agency inventories of SBU procedures, followed by the Secretary of Homeland Security along with the Attorney General, the Secretaries of State, Defense, and Energy, and the DNI developing a recommendation for standardization of all the SBU policies, and finally implementing the standardized procedures through the Office of Management and Budget (OMB). To date, no proposals have been disseminated.

METHODOLOGY

This Study seeks to evaluate the impact of the Card Memorandum directing the safeguarding of unclassified information and the breadth of policies related to the protection or control of unclassified information across the federal agencies. A number of recent reports have compiled lists of the array of different categories for non-classification protection, but none have requested and compared information from a broad swath of federal agencies on the protection of information that cannot properly be classified under existing procedures guided by the President's EO 12958. The Archive used Freedom of Information Act requests to compile data from federal agencies.

IMPACT OF CARD MEMORANDUM

On March 19, 2002, President Bush's Chief of Staff Andrew H. Card sent a memorandum ("Card Memorandum") to the heads of all executive departments and agencies of the Federal Government. The Card Memorandum called on departments and agencies to immediately reexamine current measures for identifying and safeguarding records regarding weapons of mass destruction (WMD), including chemical, biological, radiological, and nuclear weapons.

The Acting Director of the Information Security Oversight Office (ISOO) and the Co-Directors of the Justice Department's Office of Information and Privacy (OIP) prepared guidance ("ISOO-DOJ Guidance") that was attached to the Card Memorandum to assist the information reviewing process. The ISOO-DOJ Guidance examines three levels of sensitivity for government information and the corresponding steps necessary to safeguard that information. These are: 1) Classified Information; 2) Previously Unclassified or Declassified Information; and 3) Sensitive but Unclassified Information. The guidance also reminds departments and agencies to process FOIA requests for records containing WMD or national security information in accordance with Attorney General John Ashcroft's FOIA Memorandum ("Ashcroft Memorandum") of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions.

The Card Memorandum directed each department and agency to report its findings directly to the Office of the White House Chief of Staff or the Office of Homeland Security no later than 90 days from the date of the Memorandum. Agencies and departments were also instructed to contact the Department of Energy's Office of Security for assistance in determining the classification of nuclear and radiological weapons information under the Atomic Energy Act, and to contact the Justice Department's Office of Information and Privacy for assistance in applying exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified (SBU) information.

The National Security Archive ("Archive") made FOIA requests to each of thirty-five (35) federal agencies, departments and offices. The 35 agencies included the 25 agencies surveyed by the Government Accountability Office (GAO) in its 2001, 2002, and 2003 reports regarding administration of FOIA. These agencies account for an estimated 97% of all FOIA requests government-wide. The Archive also submitted FOIA requests to ten (10) additional agencies and components to which the Archive frequently submits FOIA requests. Each FOIA request asked for:

> **All records, including but not limited to guidance or directives, memoranda, training materials, or legal analyses, concerning the March 19, 2002 memorandum issued by White House Chief of Staff Andrew Card to the heads of all federal departments and agencies regarding records containing information about Weapons of Mass Destruction (WMD). Attached with this memo was a supporting memorandum by the U.S. Department of Justice and Information Security Oversight Office.**

With one exception, all requests were faxed to the central FOIA processing office of each department or agency on January 8, 2003.[10] The 20-business day statutory time limit for a substantive FOIA response expired on February 5 or 6, 2003. On February 7, 2003, after 21 or 22 business days had expired, appeals were filed with 30 agencies that had not substantively responded to the requests. The Chart presented in Appendix I summarizes agency processing times and information releases.

POLICIES ON PROTECTION OF SENSITIVE UNCLASSIFIED INFORMATION

The Archive submitted FOIA requests to each of 43 different federal agencies, departments, and offices. This survey included the 25 agencies examined by the Government Accountability Office (GAO) in its annual reports; the agencies considered by the GAO represent an estimated 97% of all FOIA requests. We selected ten additional agencies and components to which the National Security Archive submits a substantial number of FOIA requests each year, as well as eight agencies that we believed, because of the nature of their functions, might play an important role in the protection of sensitive unclassified information. Each request sought:

> **All documents including, but not limited to, directives, training materials, guides, memoranda, rules and regulations promulgated on and after January 1, 2000, that address the handling of,**
>
> **"sensitive but unclassified," (SBU)**
> **"controlled unclassified information," (CUI)**
> **"sensitive unclassified information," (SUI)**
> **"sensitive security information," (SSI)**
> **"sensitive homeland security information," (SHSI)**
> **"sensitive information," (SI)**
> **"for official use only," (FOUO)**
>
> **and other types and forms of information that, by law, regulation or practice, require some form of protection but are outside the formal system for classifying national security information or do not meet one or more of the standards for classification set forth in Executive Order 12958 as amended by Executive Order 13292.**

The requests were faxed to the central FOIA processing office of each agency or department on February 25, 2005. In some cases separate requests were submitted to component agencies that may have occasion to independently safeguard unclassified information. The 20-business day statutory time limit for a substantive FOIA response expired on March 25, 2005. The chart presented in Appendix III summarizes agency processing times and information releases.

Agency responses were examined for:

- Authority (statutory or internal) for the policy;
- Definition and guidance;
- Power to designate protected information;
- Power to remove designation;
- Government employees' access to information;
- Physical protections for information;
- Limitations on use of designation;
- Relation to or effect on Freedom of Information Act (FOIA) policies.

Each of the above categories corresponds with the explanatory sections below (*see* **Findings**). The constraints of this Report format do not allow the details of each agency policy to be communicated; instead, we have drawn generalized findings based on an overall review and used specific aspects of agency responses as examples or case studies within our broader discussion. The complete documentation of each agency's response is available on file with the National Security Archive, http://www.nsarchive.org.

What Is Sensitive Unclassified Information?

This study is focused solely on security sensitive information that does not meet the standard for classification or, for some other reason, is not classified in accordance with Executive Order 12958 (as amended by E.O. 13292). When referring generally to the category of policies examined in this Study, rather than a specific agency policy (the names of which are denoted in **bold text**), we use the term "sensitive unclassified information" policies. Because of the number of policies and the extent to which they overlap–some use the same terminology but differ in substance–this is used as a generic phrase, as it incorporates the two common elements (the claimed sensitivity of the information and its unclassified

nature). We include as "security"-related concerns those potential harms related to national security or law enforcement, as well as protection of other information the release of which may impair the functioning of the government.

What Is Not Sensitive Unclassified Information?

The web of government information control policies and practices is vast and complex. As this Study makes clear, many documents may potentially fall into multiple categories or be marked with more than one type of restriction. For purposes of clarity and focus, this Study examines specifically those policies aimed at controlling unclassified information for purposes of security. This category of information overlaps substantially with what are often referred to as "dissemination control markings"[11] or routing guidelines. Such markings may be applied to either classified or unclassified information, and serve the purpose of directing *where* a given document may go and *who* may receive it, rather than characterizing the substantive content of the document.

Examples of these "caveats" or "special handling designations" used by the Department of Defense and exclusively applicable to classified information include: ATOMAL (containing atomic materials); NATO (NATO classified information); and SIOP-ESI (Single Integrated Operations Plan-Extremely Sensitive Information) and other SPECAT (Special Category) designators.[12] The Department of State and several other agencies recognize markings specifically prescribing distribution restrictions for the document, including: EXDIS ("exclusive distribution to officers with essential need to know"); LIMDIS ("distribution limited to officers, offices, and agencies with the need to know, as determined by the chief of mission or designee"); NODIS ("no distribution to other than addressee without approval of addresser or addressee. NODIS is used only on messages of the highest sensitivity between the President, the Secretary of State, and Chiefs of Mission.");[13] and NOFORN ("intelligence which . . . may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nations, or immigrant aliens without originator approval.")[14]

NOTES ON FINDINGS

The Study's findings are qualified on a number of grounds. First, there are limitations to the method of requesting documents under the FOIA. The Archive cannot be certain that every relevant office was searched, that every responsive document was found, or that all the data on these issues was released. The wide range of responses received suggests that there almost certainly are additional responsive documents that were not provided to the Archive.

Second, as to the sensitive unclassified information policies presented in this Study, in the majority of cases, we were unable to determine to what extent these policies have affected agency practice. Due to the amorphous, decentralized, and generally unmonitored nature of policies controlling unclassified information, it is impossible to discern how many employees in a given agency are using the policy and how much information has been designated for protection or withholding under the policy. Some inferences can be drawn in cases where the means of dissemination of a given policy can be discerned, but this was not possible with the material provided by most agencies.

Third, as of today, 258 business days since submission of the FOIA request for documents on sensitive unclassified information policies, only 32 agencies out of 42 surveyed (or approximately 76%) have responded, but only 20 or 48% have provided responsive documents. In some cases, such policies are created by statute or have been pronounced publicly as agency policy. Therefore, the agency FOIA responses were supplemented with research based on publicly-available materials. Thirty-three out of 35 agencies surveyed (approximately 91%) have responded to our Card Memorandum request, but over 750 business days have passed since those requests were submitted.

Finally, there are many different tallies of the total number of sensitive unclassified information policies. Several attempts have been made to measure the volume of distinct designations used to protect unclassified information, but each organization has employed its own approach and, in particular, its own interpretation of how the boundaries of the category should be defined. In 1972, a study commissioned by the House Government Operations Committee revealed 63 separate "control labels" used by various federal agencies; however, a number of the labels included in that count are applied only as an additional safeguard to classified information–for example, Restricted Data, Siop-Esi ("Single integrated operational plan–extremely sensitive information"), and Noforn ("No foreign distribution"). Further, at least eight of the

agencies included in that survey are no longer in existence, and others are small agencies that were not included in this Study.

A more recent quantification of sensitive unclassified information policies was completed by OpenTheGovernment.org as part of their Secrecy Report Card 2005.[15] OpenTheGovernment.org referred to 50 "restrictions on unclassified information"; included in this count, however, are the nine defined exemptions under the Freedom of Information Act, as well as several other restrictions that were not reported by the agencies surveyed for this Study or that do not clearly qualify as either distribution or control markings–for example, protective measures in place under the Export Administration Regulations and restrictions applied to Grand Jury Information under the Federal Rules of Criminal Procedure. Once again, for this Study we considered principally the information and policies provided by the agencies in response to FOIA requests. The deviations as to the total number of policies exhibits two conclusions about the state of sensitive unclassified information regulation–namely, that these diverse policies are not clearly set out by the agencies or publicly available, and that there is even misunderstanding and disagreement within agencies about the nature and application of the policies.

FINDINGS

CARD MEMORANDUM AND PROTECTION OF UNCLASSIFIED HOMELAND SECURITY INFORMATION

Of the 35 FOIA requests, the Archive received 24 responses with documents. Nine departments responded that their searches yielded "no records." Finally, two departments (USAID and CIA) have not provided any formal response to the Archive's initial request after more than three years nor formally responded to administrative appeals based on their non-responsiveness. Surprisingly, seven agencies apparently did not provide a report back to Mr. Card despite his explicit direction to prepare such a report. The agency response times ranged from 9 to 702 business days. A summary of the agency processing times and document releases is attached in Appendix I.

Each agency that provided records indicated taking some action in response to the Card Memorandum and/or the ISOO-DOJ guidance. A summary of the agencies responses to the Card Memorandum is attached in Appendix II and the agencies complete responses are available on our Web site at http://www.nsarchive.org. Overall, the Card Memorandum appears to have resulted in increased withholding of information, both in the form of information removal from Web sites and increased emphasis on using FOIA exemptions. Some of the new security measures put into place at agencies, including Web site policies, appear to have been long overdue and are likely to increase the security of sensitive information.

REVIEW OF RECORDS FOR WMD OR OTHER SENSITIVE INFORMATION

At a minimum, responsive departments and agencies provided records indicating that they reviewed their records and identified whether they held WMD information. Some departments conducted much more expansive searches to identify a far broader range of potentially sensitive information, including "Sensitive Homeland Security Information" (SHSI), classified information, "Safeguard Information," "potentially sensitive information," and "other information that could be misused to harm the security of [the] nation or threaten public safety."

WEB SITE INFORMATION REMOVAL

At least ten agencies indicated that they removed information from their Web sites or blocked access to their Web sites. Several departments and agencies reported identifying WMD information, national security, and public safety information on their public Web sites. The common reaction by these departments and agencies upon identifying this information was to immediately remove the information or begin the bureaucratic process of removing it. This number almost certainly underestimates the number of agencies that removed data from Web sites post-September 11, as many agencies, such as the Nuclear Regulatory Commission, began closing access to online information prior to receiving the Card Memorandum.

Individual approaches to identifying information on Web sites and making the decision to remove the information varied. A few responses indicated that special task forces or teams were created to inventory Web sites, identify sensitive information on the sites, and to assess whether the information should be removed. Some agencies had teams immediately remove all sensitive information from public Web sites and then either used those same teams or other individuals, including FOIA officers or other authorized personnel, to determine what information could be reposted. Additionally, a number of agencies created specific protocols or policies for posting future potentially sensitive content on public Web sites.

Some agencies used the review as an opportunity to increase cyber-security by installing firewalls, conducting vulnerability scans on Web sites, and enhancing access restrictions.

INCREASED EMPHASIS ON USING APPLICABLE FOIA EXEMPTIONS

At least 16 of the 24 agencies that responded provided records that demonstrated an increased emphasis on using FOIA exemptions to withhold information. Several agencies that would be expected to hold or handle WMD or other sensitive information emphasized to FOIA officers that they should use careful consideration in determining the applicability of all FOIA exemptions when processing a request for sensitive information, often citing verbatim the language and instruction of the ISOO-DOJ guidance. For example, the Office of Security in the Energy Department generated: a list of "Subject Area Indicators and Key Word List for Restricted Data and Formerly Restricted Data" and an "Interim Guide for Identifying Official Use Only Information." These lists include scientific terms, sites, or organizations associated with Restricted Data and Formerly Restricted Data, frequently encountered names of people involved in Nuclear Weapons Programs, and "possible markings." These lists presumably will be used by FOIA officers to help determine the applicability of FOIA exemptions to records containing one or more of the words on the lists. The "Interim Guide" emphasizes usage of all FOIA exemptions and offers examples of situations in which a particular FOIA exemption could be applied.

In addition, some agencies either employed additional review of FOIA requests or developed new procedures. For example, a joint DOD response indicates a decision that any Chemical, Radiological, Biological, and Nuclear (CBRN) is found subject to declassification, then it must be approved by Washington Headquarters Services, Directorate of Freedom of Information and Security Review (WHS/DFOISR). DFOISR planned to issue a change to DoD Directive 5230.29 to require CBRN to be referred to DFOISR before public release of such information.

Several agencies implemented ongoing training programs or training sessions for FOIA officers to ensure future compliance with the ISOO-OIP Guidance.

Only two agencies provided statements to balance out any increased emphasis on withholding. In a memorandum disseminating the Card Memorandum and ISOO-OIP Guidance, the EPA informed its offices that no EPA policies were changed as a result of the memoranda and indicated that EPA offices should recognize both the risks and the benefits of disclosure. Similarly, DOD provided records indicating that safety should be considered alongside the benefits associated with the free exchange of information.

IMPLEMENTING NEW SECURITY AND SAFEGUARDING MEASURES

Several agency responses indicated that the agencies implemented new security and safeguarding measures. For example, the Department of Agriculture commenced parallel in-house and external reviews of its most sensitive research laboratories, with a major focus of the reviews being "human reliability" and "information security." In addition, the Department "ramped up" its department-wide personnel security and information security programs by "increasing the budget for personnel security investigation and adjudications several-fold" and "drafting an updated departmental regulation on protecting national security information."

DISSEMINATION OF CARD MEMORANDUM

Agencies that would not be expected to handle WMD information or other sensitive information, in some cases, simply forwarded the Card Memorandum and the ISOO-DOJ guidance to its FOIA offices in a "for your information" manner.

NO RECORDS OR NO RESPONSE

Nine agencies responded that they held no documents responsive to the Archive's FOIA request. Those agencies include: (1) Social Security Administration; (2) Office of Management and Budget; (3) Department of Housing and Urban Development; (4) Department of Health and Human Services (HHS); (5) Federal Bureau of Investigation (FBI); (6) Department of Education; (7) Defense Intelligence Agency (DIA); (8) Office of Personnel Management (OPM); and (9) Central Command (CENTCOM). Since the Card Memorandum *required* each agency to submit a report to either the Office of the White House Chief of Staff or to the Office of Homeland Security, these agencies either failed to release their reports to the Archive or failed to submit the report requested by Mr. Card. Two agencies, CIA and AID, have not provided any substantive response, despite administrative appeals by the Archive.

For those agencies that do not deal with military or intelligence issues, it is not surprising that the Card Memorandum did not result in much activity, including possibly the failure to submit a formal response to the White House Chief of Staff or the Office of Homeland Security. Other "no records" responses raised questions, however. For example, although HHS reported holding no documents responsive to the Archive's request, the HHS Web site shows that the department, particularly through the Center for Disease Control (CDC), disseminates information regarding biological, chemical, and radiological weapons.

AGENCY CONTROL OF SENSITIVE UNCLASSIFIED INFORMATION

AUTHORITY FOR POLICY

The agencies and departments examined in this study present a broad range of varied approaches to protecting information that is not subject to security classification. The authority for these diverse policies ranges from an agency's inherent information management authority to specific statutory direction. It is striking to note the multiplicity of policies and terms that agencies have created internally to apply to unclassified information, as compared to the relative simplicity and perceptible origins of statutorily-authorized policies. The "patchwork quilt" of guidelines related to sensitive unclassified information is made up primarily of squares sewn with agency–rather than congressional–threads.

I firmly believe that never before have we had such a clear and demonstrable need for a seamless process for sharing and protecting information, regardless of classification. Yet in many ways, we are not only continuing the current 'patchwork quilt' but we are quite possibly adding new seams every day.
– J. William Leonard, ISOO Director[xi]

Agency-Originated Policies

Of the 37 agencies surveyed (both by way of responses to our requests as well as by outside research, see chart at Appendix III), 24 follow one or more different internally-generated policies (in some cases, an internal agency policy statement will draw on the definition and criteria in a statute or another agency's policy) to protect information that is considered "sensitive" for security reasons. In general, because of their less formal nature, these policies are less restrictive in terms of which employees or officials may mark sensitive information and are more expansive in terms of what information may potentially be covered. Definitions tend to be less precise or concrete in their application than statutorily-authorized policies.

24 out of 37 of agencies and departments analyzed (65%) protect certain types of unclassified information originating within the agency according to *internal* policies, procedures, or practices.

Some of the materials provided regarding these agency-generated policies consist of formal orders or directives establishing agency policy and procedures; in other cases, particularly those agencies that have little involvement in security matters, the policies are contained within employee handbooks or manuals, or even training materials such as pamphlets and Power Point presentations assumedly targeted to provide essential but simplified background to new employees or security trainees. Unfortunately, it is impossible to reach any conclusions as to the extent of use or dissemination of the policy based on the form or content of these documents.

It is clear from the multiplicity of internal policies that there has been no coordination among agencies as to the content of the policies. This is also particularly evident in the fact that many of the agencies use the same terms or markings for their policies, but control, monitor, and release designated documents according to very different guidelines.

AGENCY-ORIGINATED POLICIES	
Agency	**Policy**
Agency for International Development (AID)	Sensitive But Unclassified (SBU)
Centers for Disease Control (CDC) *	Sensitive But Unclassified (SBU)
Citizenship and Immigration Services (CIS) *	Sensitive But Unclassified (SBU) [DHS]
Customs and Border Protection (CBP) *	Sensitive But Unclassified (SBU) [DHS]
Department of the Air Force ("Air Force") *	For Official Use Only (FOUO) [DOD]
	Computer Security Act Sensitive Info [DOD]
Department of Agriculture ("USDA")	Sensitive Security Information (SSI)
Department of the Army ("Army") *	For Official Use Only (FOUO)
Department of Defense (DOD) *	For Official Use Only (FOUO)
Department of Energy (DOE)	Official Use Only (OUO)
Department of Homeland Security (DHS)	Sensitive But Unclassified (SBU)
Department of Justice (DOJ)	Limited Official Use (LOU)
Department of State (DOS)	Sensitive But Unclassified (SBU)
Department of the Treasury ("Treasury")	Sensitive But Unclassified (SBU)
Drug Enforcement Agency (DEA)	DEA Sensitive
Environmental Protection Agency (EPA)	Confidential Agency Information (CAI)
	Confidential Business Information (CBI)
	Enforcement-Confidential Information (ECI)
Federal Aviation Administration (FAA)	For Official Use Only (FOUO)
General Services Administration (GSA)	Sensitive But Unclassified Building Info
Immigration and Customs Enforcement (ICE) *	Sensitive But Unclassified (SBU) [DHS]
National Aeronautics and Space Admin. (NASA)	Administratively Controlled Info (ACI)
National Geospatial-Intelligence Agency (NGA)	For Official Use Only (FOUO) [DOD]
National Reconnaissance Office (NRO)	For Official Use Only (FOUO)
National Science Foundation (NSF)	Sensitive Information
Nuclear Regulatory Commission (NRC)	Official Use Only (OUO)
	Proprietary Information (PROPIN)
Transportation Security Administration (TSA)	Sensitive But Unclassified (SBU) [DHS]

***** The information was not provided by this agency, but rather is based on independent research or materials submitted by other agencies.

Statutory and/or Regulatory Policies

Of the agencies analyzed, eight follow one or more statutory guidelines applicable to unclassified information. Two of these agencies–the Department of Energy and the Nuclear Regulatory Commission–have long-standing policies, based on the Atomic Energy Act of 1954. The remaining statutory policies were created or restructured from previous enactments by the Homeland Security Act of 2002. They include:

8 out of 37 agencies (22%) analyzed have policies that are authorized *by statute* and implemented *by regulation*.

Authorization for 2 policies is derived from the Atomic Energy Act of 1954; 5 rely on the Homeland Security Act of 2002; and 3 are based on other statutory pronouncements or regulatory authority.

- **Sensitive Security Information (SSI)**

  Sensitive Security Information (SSI) related to civil aviation has been statutorily safeguarded for more than three decades under the Air Transportation Security Act of 1974. It was initially intended to prevent airplane hijackings. These provisions have been expanded under the Homeland Security Act. New authority to withhold information has been extended to the Under Secretary of Transportation for Security and authority has been extended to the TSA and the DHS. The **SSI** restrictions

are now applicable to all transportation information and to maritime-related security information under the jurisdiction of the Coast Guard.

- Protected Critical Infrastructure Information (PCII)

  The Department of Homeland Security (DHS) issued regulations in 2004 based on provisions of the Homeland Security Act, creating its Protected Critical Infrastructure Program. The program applies to **"critical infrastructure information" (CII)**–information "not customarily in the public domain and related to the security of critical infrastructure or protected systems," which, if sabotaged, attacked, or otherwise impeded, would result in the incapacitation of interstate commerce, national security, or public health or safety–that is voluntarily submitted to DHS by private sector entities. A new office established within DHS will handle applications connected to the submission of **CII**, and will grant **PCII** status if certain conditions are met; once designated as **PCII**, this information will be withheld on FOIA exemption 3 grounds.[16]

- Sensitive Homeland Security Information (SHSI)

  The 2002 Act defines **"homeland security information" (HSI)** as "Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist attack."[17]

  The President is granted authority to safeguard homeland security information–that which is classified as well as that which he deems to be "sensitive but unclassified." The statute outlines the ways in which this type of information should be shared among federal, state, and local officials and personnel, including in particular, "[w]ith respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel."[18]

  President Bush delegated to the Secretary of Homeland Security the task of promulgating procedural regulations to comply with the statutory provisions. DHS has yet to issue formal proposed regulations implementing the SHSI provisions of the Homeland Security Act.

STATUTORY POLICIES		
Agency	**Policy**	**Statutory/Regulatory Authority**
AIR	Sensitive Information	Computer Security Act of 1987, P.L. 100-235
DHS	Sensitive Security Information (SSI)	49 U.S.C.A. § 40119 49 C.F.R. § 1520.5
	Protected Critical Infrastructure Information (PCII)	Homeland Security Act of 2002, 6 U.S.C.A. § 131 6 C.F.R. § 29
DOD*	Unclassified Controlled Nuclear Information (UCNI)	10 U.S.C.A. § 128 32 C.F.R. § 223
	Sensitive Information	Computer Security Act of 1987, P.L. 100-235
DOE	Unclassified Controlled Nuclear Information (UCNI)	Atomic Energy Act of 1954, 42 USCA § 2011 10 C.F.R. §1017.7
FAA/ DOT	Sensitive Security Information (SSI)	Air Transportation Security Act of 1974 Homeland Security Act of 2002, 6 U.S.C.A. § 101 49 C.F.R. Part 15.5
NRC	Safeguards Information (SGI)	Atomic Energy Act of 1954, 42 USCA § 2167 10 C.F.R. § 73.21
TSA	Sensitive Security Information (SSI)	49 U.S.C.A. § 40119 49 C.F.R. § 1520.5
	Protected Critical Infrastructure Information (PCII)	Homeland Security Act of 2002, 6 U.S.C.A. § 131 6 C.F.R. § 29

***** The information was not provided by this agency, but rather is based on independent research or materials submitted by other agencies.

No Policies

Most of the agencies that interact on an individual level with the citizens they serve do not maintain SBU or similar information-control policies. In other cases, those agencies that deal extensively with the federal budget and other matters that are generally part of the public domain would not have a need for such a policy.

11 of the agencies that responded provided *no documents* showing a policy for protecting security-related sensitive information. They include:

- **Social Security Administration (SSA)**
- **Small Business Administration (SBA)**
- **Office of Management and Budget (OMB)**
- **Federal Emergency Management Agency (FEMA) – *Fwd. to DHS***
- **Department of Housing and Urban Development (HUD)**
- **Office of Personnel Management (OPM)**
- **National Institutes of Health (NIH)**
- **Department of Commerce ("Commerce")**
- **National Archives and Records Administration (NARA)**
- **Department of Veterans' Affairs (VA)**
- **Federal Bureau of Investigation (FBI)**

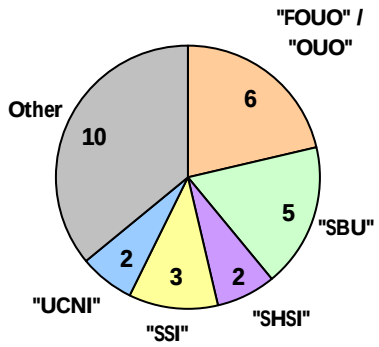
DEFINITION AND GUIDANCE

This Study analyzed the specificity and extent of guidance given to individuals who are to designate or mark protected information under the policy. The research revealed 28 *distinct* policies related to sensitive unclassified information,[19] and the various policies were grouped according to what type of definition or guidance was provided in the policy statement or other procedural document. The definitional features considered were whether the policy relies on a broad/specific definition; delineated categories/criteria of information to be protected (broad or specific); examples of agency-specific materials to clarify either a definition or set of categories; and any other statutory guidance to which the policy refers, for example, one or more of the nine exemptions under FOIA, 5 U.S.C. §552(b). See charts, Appendices IV and V.

This Study examined 28 *distinct* policies prescribing treatment of sensitive unclassified information.
Of these 28 policies,

- **6 refer to protected information as "For Official Use Only" (FOUO/OUO);**
- **5 as "Sensitive But Unclassified" (SBU);**
- **2 as "Sensitive Homeland Security Information" (SHSI);**
- **3 as "Sensitive Security Information" (SSI); and**
- **2 as "Unclassified Nuclear Information" (UCNI).**

Sensitive Unclassified Information Labels, 28 Distinct Agency Policies



The degree of guidance offered is an essential consideration in our analysis of these policies because it shows to what extent government officials (and, in some cases, low-level employees) are constricted in their decision to mark information for protection. Facing challenges to its SSI policy in 2004, the TSA Internal Security Policy Board concluded: ". . . [E]xacting specificity with respect to what information is covered and what is not covered. . . . could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining **SSI**. Experience has shown that employees unsure as to what constitutes **SSI** may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure."[20]

"Sensitive but unclassified information is a very imprecise term that has more often than not been misunderstood. It might refer to information that should be protected from public disclosure, or should be safeguarded, or both."
- J. William Leonard, ISOO Director[xii]

More constrained, specific policy guidance—as opposed to broad, general criteria or categories—allows for only a narrow range of interpretation and prevents misunderstanding or abuse of the policy.

In comparison to the strict, detailed principles of the national security classification regime, the formal categories and criteria in protective markings for unclassified materials are often sparse, inconsistent, and ambiguous. Because, as ISOO Director J. William Leonard has highlighted, "[t]here is no underestimating the bureaucratic impulse to 'play it safe' and withhold information,"[21] the poor guidance in many cases may presage poor decision-making, or at least increase the likelihood that secrecy by default will become the rule rather than the exception.

FOIA-Based Definitions

In a number of agencies, FOIA exemptions two through nine are transposed into sensitive unclassified information policies by way of definition. The potential for conflating the statutorily defined FOIA exemptions with broader notions about potentially sensitive information is significant. For instance, the State Department manual, 12 FAM 540, defines SBU as "information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under . . . the Freedom of Information Act and the Privacy Act." The provision goes further to illustrate what information is covered, explaining: "**SBU** information includes, but is not limited to . . . [m]edical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations."

Other FOIA-based definitions—the Department of Defense **FOUO** information, for example—expressly limit protected information to that which is subject to withholding under the FOIA exemptions. The problem with this approach is that the goal of FOIA is disclosure, while the goal of SBU-type policies is information safeguarding or non-disclosure. It is important that sensitive unclassified information designations not be seen as determinant of FOIA releasability, particularly because FOIA release decisions for the same documents may change over time. Especially where these policies can be invoked by *any employee*, it is acutely important that their scope and purpose be limited to avoid potential misuse and excessive secrecy. The one benefit of FOIA-based definitions, however, is that there are statutory definitions and a body of administrative and public law interpreting those definitions. Nonetheless, it remains imperative that FOUO not be considered a FOIA exemption.

Definitions Versus Categories

In most cases, agency policies include a definition, which is often broad or circular in terms of describing the information to be protected. For example, the Department of Justice authorizes selected personnel to designate agency information as **"Limited Official Use" (LOU)**; **LOU** is defined as "[u]nclassified information of a sensitive, proprietary or personally private nature which must be protected against release to unauthorized individuals." (DOJ 2620.7). Like a number of other agencies, DOJ's policy lists the types of information that fit under this definition, some very narrow and statutorily defined—for example, Grand Jury information and Privacy Act-protected information—and some vague and open-ended—"Reports that disclose security vulnerabilities" and "Information that could result in physical risk to individuals."

The status of sensitive information outside of the present classification system is murkier than ever. . . . 'Sensitive but unclassified' data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used."
– JASON Program Office, MITRE Corp.[xiii]

Several other policies describe sensitive information broadly in terms of national security or general governmental interests. DHS permits *any employee* (the agency is now the largest in the Federal Government, with more than 180,000 employees) to mark a document "FOR OFFICIAL USE ONLY" if they consider that its contents "could adversely impact . . . the conduct of Federal programs, or other programs or operations essential to the national interest." This directive is further clarified with 9 sub-categories, including, among others: "Information that could be sold for profit";

"Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security"; and "Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasures, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system." (DHS Management Directive 11042.1)

Some of the policies surveyed for this project, to their credit, offer extremely narrow and well-delineated categories, such that it would be very difficult for employees applying the policy to mistakenly conclude that a document does or does not need protection. The Nuclear Regulatory Commission, in an internal memo to senior officials, directs that Safeguards Information must be withheld from public release; the guidance includes such materials related to nuclear facilities as: "Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system"; "Details of the onsite and offsite communications systems"; "Lock combinations and mechanical key design"; "Size, armament, and disposition of onsite reserve forces"; and "Schedules and itineraries for specific shipments."

It is relevant to note that NRC's SGI policy has been in effect since 1981 (although the agency proposed new regulations in February 2005 that would expand the existing definition). This change would add a new category of Safeguards Information-Modified Handling (SGI-M) to cover many security and emergency planning procedures and particular types of safety assessments regarding nuclear facilities. This example exhibits the problematic though critical difference between information control procedures before and after September 11: namely, the United States has recognized the extent of its ignorance about the precise threat posed by terrorists and through what means a potential future strike might occur. Given this uncertainty, the Government has thrown an increasingly wide net of protection over information in the hope that the right secrets will be kept to avert another attack.

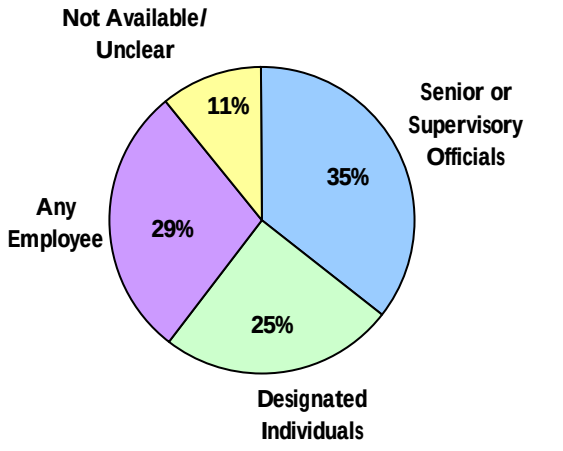
"[T]hose making SSI designation . . . should have special training, much as FOIA officers do, because they are being asked to make difficult balancing decisions among competing values. All of us value security, but any security gained from the regulations is of considerably less comfort if it comes with a loss of faith and confidence in our local, state and national governments to safeguard our other values."
- Coalition of Journalists for Open Government[xiv]

DESIGNATION AUTHORITY

Each agency policy was examined for how it delegates the authority to determine what is (and what is not) protected material. In a handful of cases, the policies were distressingly ambiguous or did not explicitly delegate this role to any particular individuals. It may be that further procedural or practical steps taken by the agencies in this regard are not reflected in the documentation provided. When a policy was ambiguous in a way that suggested intentional breadth and was apparently intended to target a broad, agency-wide audience, this Study concludes that any agency personnel has the authority to act according to its dictates.

Clearly, individuals who are authorized to designate (rather than just to view or possess) materials as protected have great power in terms of the impact of the policy, both for dissemination of information within the agency or the government (information sharing) and access of the public to government information. In particular, with the newest policies–those instituted or revamped since September 11–more agencies are ambiguous in their selection of responsible employees. Other agencies explicitly have assigned the designation role, but to a group of employees that is arguably so large as to make training or oversight impractical unless directed at the entire agency staff.

Authority to Designate Protected Information



Recently, during consideration of the Department of Homeland Security Appropriations Act, 2006, the congressional Conference Committee specifically addressed

the use of the **Sensitive Security Information (SSI)** designation, particularly within components of DHS including the Transportation Security Administration (TSA). In its report, the Committee stated:

> The conferees are concerned that because of insufficient management controls, information that should be in the public domain may be unnecessarily withheld from public scrutiny. The conferees require the Secretary to ensure that each appropriate office has an official with the clear authority to designate documents as **SSI** and to provide clear guidance as to what is **SSI** material and what is not.[22]

The solution that the congressional committee proposes—requiring each office, department, or division to select a single individual to whom they delegate the responsibility of marking, reviewing, and disseminate those documents that are "sensitive" or otherwise protected—is one that seven (7) agencies already follow.

Several other agencies have taken an approach that is effectively a two-step process for designation. A senior-level official or other designated authority will first have the task of implementing the stated policy and by indicating particular *categories* or *types* of information that should be protected within the agency or department. Based on this list of specific criteria that constrain decision-making, other employees will then be able to mark and protect particular information they produce according to the guidelines. The **Department of Homeland Security's FOUO** policy takes this approach. The DHS policy has been widely criticized for its breadth, but in actuality may be more nuanced in its controlled application: "Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited. . . . Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO." (DHS MD 11042.1). The clarity of the stated categories is debatable, as noted above, but they undoubtedly narrow a much larger scope of information that could fall within the definition of FOUO and avert the potentiality of haphazard, unguided application that might otherwise exist.

Similarly, the Department of Energy (DOE) has written its policy in such a way that the terms can evolve based on high-level guidance as the agency's needs change over time. The **DOE OUO** policy includes as a responsibility of both Secretarial Officers and the Director of the Office of Security to issue guidance "to assist individuals in determining whether a document contains **OUO information**." Employees may mark a document from their office as **OUO** if they determine that "the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities"; *and* if the information contained therein either is specifically identified as **OUO** information under the official guidance *or* if they believe the information otherwise qualifies for protection under FOIA exemptions 2 through 9.

AUTHORITY TO *DESIGNATE* PROTECTED INFORMATION	
Senior or supervisory officials **10 of 28 (35%)**	ACI / NASA ("originating NASA management official") DEA Sensitive ("senior official") FOUO / FAA ("FAA managers") OUO / NRC ("Branch chiefs and above" and contractor-appointed) SBU / State ("US citizen direct-hire supervisory employees") SSI / DOT SGI / NRC ("Branch chiefs and above") SSI / USDA ("Heads of Departmental Organizations") UCNI / DOD ("Heads of DoD components") Unclassified Technical Info / DOD
Designated individuals **7 of 28 (25%)**	LOU / DOJ ("designate[d] subordinate officials") PCCI / DHS SASI / HHS SBU / CDC ("Document control officers") SHSI / FAA ("SHSI Program Officer") SHSI / NRC (staff assigned as "points of contact" for SHSI) UCNI / DOE ("Reviewing Official")

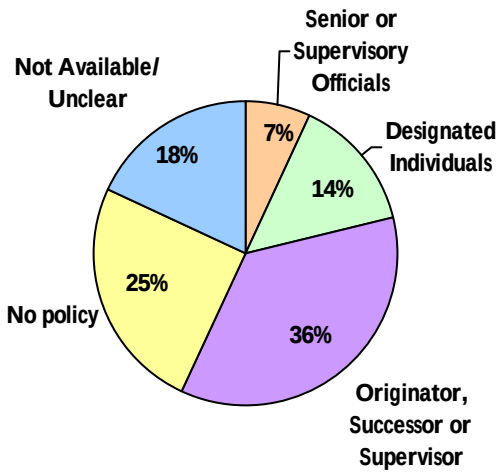
Any employee **8 of 28 (29%)**	CAI/EPA ("originator or information manager") CBI/EPA ("originator or information manager") ECI/EPA ("originator or information manager") FOUO/DHS ("An y DHS employee, detailee, or contractor") FOUO/DOD FOUO/NRO ("Originator of info") OUO/DOE ("Any Federal or contractor employee" originating/controlling document) SBU/GSA
Not available / unclear **3 of 28 (11%)**	Computer Security Act Sensitive/DOD PROPIN/NRC WMD/State

DECONTROL AUTHORITY

This Study inquired as to whether each policy sets forth a procedure for removing a protective marking or otherwise sharing or disseminating the information after it has previously been controlled under one of the subject policies. In addition, whether or not such a process was outlined, this Study looks at whether the policy identifies an individual or individuals authorized to effectively erase a protective stamp from a sensitive unclassified document and thereby release it from safeguarding measures.

The comparison between the identification of a designating authority and of decontrol authority speaks loudly as to the breadth and indeterminate nature of these policies. In fact, the contrast proves stark. While only three out of 28 policies (11%) *do not* clearly identify specific authority to designate information for protection, 12 of the same 28 policies (43%) either were examined in their entirety and clearly provided no guidance on decontrol or were incomplete or ambiguous as to establishing a decontrol procedure or authority. Further, although several agencies name individuals responsible for decontrol, none has mandatory review or tracking policies for decisions to protect unclassified information, and only one has a time limit (USDA, 10 years) and few have other restrictions on the use of these designations. In a majority of agencies, the only opportunity for review of a document designated for protection is when the information is requested under the FOIA. At this point, there are different procedures for how an agency will handle such a request, which will be discussed below.

Authority to Decontrol Protected Information



Some of the policies designate a removal authority—in many cases limited to the individual who placed the original designation (or his or her successor or superior). Without any mandated review, however, any examination or removal of markings (whether by the document's originator or other specified authority) will inevitably be completed in a haphazard manner. NASA's **Administratively Controlled Information (ACI)** policy, for example, states that the "[o]fficial who originally designated material as **ACI** (or successor or superior) are responsible for prompt removal of restricted markings when the necessity no longer exists." Without knowing the extent of the paper that one individual official may imprint with the "ACI" stamp on a daily basis but considering the nature of the federal bureaucracy, one questions how an already-burdened NASA management

official will be capable of paging through his or her filing cabinets to make sure the status of each document has not changed.

The least common approach is to follow the pattern of the classification system, mandating a maximum duration for protective marking. At USDA, "[i]nformation shall not remain protected as **SSI** when it ceases to meet the criteria established in sections 6.b of this regulation. Information ordinarily should remain protected as **SSI** for no longer than 10 years, unless a designating official makes a new determination the protection is warranted for a longer period." (USDA, DR 3440-2).

AUTHORITY TO *DECONTROL* PROTECTED INFORMATION	
Senior or supervisory officials **2 of 28 (7%)**	SSI / USDA, *maximum 10 years* Unclassified Technical Info / DOD
Designated individuals **4 of 28 (14%)**	PCCI / DHS SASI / HHS SBU / CDC ("Document control officers") SHSPI / FAA ("SHSI Program Officer")
Originator or successor / supervisor **10 of 28 (36%)**	ACI / NASA ("originating NASA management official") FOUO / DHS ("Any DHS employee, detailee, or contractor") FOUO / DOD FOUO / FAA ("FAA managers") FOUO / NRO ("Originator of info") – with senior authorization OUO / DOE ("Any Federal or contractor employee" originating / controlling document) OUO / NRC ("Branch chiefs and above" and contractor-appointed) PROPIN / NRC SGI / NRC ("Branch chiefs and above") UCNI / DOE ("Reviewing Official")
No policy provided **7 of 28 (25%)**	CAI / EPA ("originator or information manager") CBI / EPA ("originator or information manager") ECI / EPA ("originator or information manager") SBU / State ("US citizen direct-hire supervisory employees") SBU / GSA SHSI / NRC (staff assigned as "points of contact" for SHSI) UCNI / DOD ("Heads of DoD components")
Not available / unclear **5 of 28 (18%)**	Computer Security Act Sensitive / DOD DEA Sensitive ("senior official") LOU / DOJ ("designate[d] subordinate officials") SSI / DOT WMD / State

GOVERNMENT EMPLOYEES' ACCESS TO PROTECTED INFORMATION

All of the agency policies included some limit on who may have access to protected unclassified information, both within the agency itself and among agencies, government contractors, and other federal (and in some cases state and local) government offices. In all cases, the provision involved some variation of a "need-to-know" requirement. The intention of applying this general principle is to minimize distribution and duplication of protected materials, by allowing them to circulate only when necessary for government business.

The most common specific definition of "need-to-know" refers to those individuals who need the specific information to perform their official duties or other agency-authorized activities. In most cases, these individuals can be government employees or contractors who require access to particular sensitive information in order to do their job. Some agencies also express this restriction as a limitation on access for job-related endeavors or "government business." One example, part of the State Department policy, permits that: "Employees may circulate **SBU** material to others, including Foreign Service nationals, to carry out an official U.S. Government function if not otherwise prohibited by law, regulation, or interagency agreement." (Department of State, 12 FAM 540).

Legally ambiguous markings, like sensitive but unclassified, sensitive homeland security information and for official use only, create new bureaucratic barriers to information sharing. These pseudo-classifications can have persistent and pernicious practical effects on the flow of threat information.
– Rep. Christopher Shays[xv]

Some variation can be seen in the specification of who may decide that another individual possesses the requisite need-to-know. In a number of cases, the policies grant this responsibility to "the person in possession of the document," (for example, in **Energy's OUO policy**) which could assumedly refer to any employee who either originated the document or has previously been recognized as having a need-to-know its contents. The authority to disseminate protected information presumably also bestows a more general duty to protect the information in accordance with the applicable policy. NRO, for example, states in its policy that "individuals possessing **FOUO information** must ensure the information is only disclosed or revealed to people who need the information to conduct business on behalf of the NRO." Similarly, **USDA sensitive security information (SSI)** may be distributed based on a "determination made by an authorized holder of SSI that a prospective recipient requires access to that SSI in order to perform or assist in a lawful and authorized governmental function." (USDA Departmental Regulation 3440-2).

Several agencies also place additional, although relatively minor, conditions on access to protected unclassified information. The most common condition is a specific mandate of a security background check, although it is important to note that none of the policies in question require authorized possessors of the information to have a security clearance, which is generally required to handle classified information. Agencies that require some form of background check include: AID and State (need-to-know access is "permitted only after individuals are granted a favorable background investigation"); Nuclear Regulatory Commission (access requires "determination of trustworthiness" (e.g. background check). The Department of Defense (DOD) in its policy on **Unclassified Controlled Nuclear Information (UCNI)** also enunciates specific limitations based on citizenship or position: only U.S. citizens who are government or contractor employees or members of the armed forces are granted general authorization for others, while exceptions for non-citizens to access the information are provided in certain specific situations.

In a few cases, agencies have required contract agreements or other signed notices to protect the integrity of documents designated as sensitive. Current GSA policy regarding **Sensitive but Unclassified Building Information** states that the holder of such information "must assure that recipient is an authorized user and completes Document Security Notice." In 2004, however, the Department of Homeland Security came under fire when it instituted a requirement that all of its 180,000 employees and contractors sign three-page forms, as a condition of their employment, that prohibit them from publicly disclosing **SBU information**. The policy, announced in May, threatened administrative or disciplinary action and potentially criminal or civil penalties for employees who violated the agreement. In addition, the agreement stated that signers agreed to consent to compliance searches by government inspectors "at any time or place."[23] In January 2005, after months of criticism from civil liberties groups, unions representing federal workers, and congressional members and staff (some of whom had been asked to sign the agreements in order to gain access to certain department information, but refused to so), DHS repealed the policy.[24]

"[T]hese designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."
-- Moynihan Commission Report[xvi]

Since September 11 in particular, information dissemination has been as much a critical part of our national security as has protecting secrets from potential enemies. The Homeland Security Act of 2002 imposes upon the President not just the

obligation to protect potentially sensitive information about infrastructure and security, but more importantly to facilitate the sharing among federal, state, and local officials such information that is relevant and important to security efforts.[25] This recommendation was enunciated clearly by the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"), which emphasized the role of communication and disclosure over that of protection and secrecy in the post-September 11 political climate: "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge. . . . The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network.'"[26]

PHYSICAL SAFEGUARDS FOR SENSITIVE INFORMATION

Although each policy analyzed has specific and distinct instructions (or lack thereof) for the treatment and safeguarding of subject information, most of the policies are similar in many ways and contain protective restrictions or requirements for each of several categories of different activities and uses of information. In evaluating the levels of protection and control measures proscribed, this study looked at how the policy dictated that information–both physical materials and electronic information–should be marked, stored (both during work hours and non-work hours), transmitted, and destroyed.

The chart below summarizes representative examples of different levels of protection that agencies may apply to protected unclassified information. Each agency may not have identical procedures, but this list is useful in understanding the general approach of most agencies. Note that the vast majority of policies examined (25 out of 28, or 89%) contain what will be labeled as "moderate" protective measures, with only slight variation among the categorized approaches. While this approach does serve to illuminate proscribed procedures–which are, in most cases, clearer and more expansive than the rest of the agency policies–it is important to keep in mind that this compendium does not reflect the *actual practice* within the agencies. [27]

SAFEGUARD PROCEDURES			
	Low/Non-specific	**Moderate**	**High**
Storage			
Work hours	- "Adequately safeguarded," "reasonable care to limit unauthorized dissemination" (LOU/DOJ) - Balancing: value of info and probability of adverse impact from disclosure (Sensitive/DOD)	- Keep in access-controlled space - No entry by unauthorized persons	- Locked security storage container (steel filing cabinet, safe deposit box) when unattended
Non-work hours		- Secure container (locked desk, file cabinet, office)	- Locked security storage container (e.g. steel filing cabinet, safe deposit box)
Electronic		- Password-protect file - No storage on public networks, if possible	
Transmission			
Physical	- Ordinary mail	- Opaque envelope; - USPS or commercial	- Opaque cover, marked; - Government/contract messenger
Electronic	- Use discretion on phone; - Follow standard computer security policies	- Include marking; - Secure phone/fax when available - Encrypted email when available	- Secure or encrypted communications systems at all times

Destruction			
Physical	- Tearing - Other (to prevent access)	- Tearing, - Shredding, - Burning	- Shredding, - Burning, - Pulping, - Chemical decomposition
Electronic		- Destroy/erase electronic media and back-up copies	
Marking			
	- No specific marking requirement; - Should carry distribution restriction		

LIMITATIONS ON USE OF INFORMATION CONTROLS

Only 7 out of the 28 policies (25%) include an explicit stipulation against the misuse for improper purposes of the information control measures contained therein.

The following qualifiers are examples of the types of cautionary or prescribed restrictions included in several of the policies:

- "Information must not be designated as **Sensitive Security Information (SSI)** to conceal violations of law; inefficiency; administrative error; prevent embarrassment to a person, organization, department or agency; or restrain competition." (Department of Agriculture)
- "No other material shall be considered **FOUO** and **FOUO** is not authorized as an anemic form of classification to protect national security interests." (Department of Defense)
- "By designation, **FOUO** is used solely for official purposes, which generally precludes work at a residence or other non-official location." (National Reconnaissance Office)
- "Information must not be designated as **Limited Official Use** to conceal inefficiency, misdeeds or mismanagement." (Department of Justice)
- "Information shall not be designated as **FOUO** in order to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency." (Department of Homeland Security)

It is important to note that of these stated restrictions, all except one are part of policies that were in place prior to September 11. Only the Department of Homeland Security, which as an entity came into being in January 2003, has a newly-crafted qualifier. This restriction is particularly important in the case of DHS, however, as the FOUO marking can be applied by *any employee* of DHS, and so is potentially open-ended and subject to abuse more so than other, more specific policies.

Certainly this type of precise limitation is highly important as a means to alert employees and officials subject to the policy how it should, and should not, be used. Various aspects of these policies governing the protection of sensitive unclassified information certainly present a risk of abuse or misapplication. Although our research does not show to what extent qualifiers or explicit restrictions on these policies actually influence decision-making, nor does it describe what if any punishment might follow from employees' failure to heed such warnings, it is instructive to review the small number of provisions that at least on the surface seek to control the rampant protection of unclassified documents.

UNCLASSIFIED INFORMATION POLICIES AND THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) is inevitably intertwined with agency policies related to the protection, control, or non-disclosure of government information. Thus, policy changes within the Executive Branch (and in some cases initiated or supported by Congress) regarding the control of sensitive information can affect public access to information under the FOIA.

A majority of the agencies surveyed include in their policies some reference to FOIA. In certain cases, the FOIA is incorporated as a *definition of* protected information. At the other extreme, certain agency policies declare conclusively that a particular category of protected information fits within one or more of exemptions under the FOIA, and therefore suggests, encourages, or mandates withholding under that exemption unless review determines disclosure to be appropriate under FOIA policy. Some agencies stipulate an ordinary review of protected information under the FOIA before release, and in such cases, the sensitive designation ought not change the status of a document in the FOIA context. Others, however, place supplemental limitations on disclosure of protected information under FOIA, ranging from a requirement of specific authorization from high-level officials for each document to a policy of standard withholding of particular types of information under a specified exemption(s).

As a final note, agencies should be aware that although various government agencies today might use newly created terms to refer to categories of homeland security-related information–such as "Sensitive Homeland Security Information" (commonly referred to as "SHSI"), "Sensitive But Unclassified Information" (sometimes referred to as "SBU information"), or "Critical Infrastructure Information" (commonly referred to as "CII")–these categorical labels do not indicate classification pursuant to Executive Order 12,958. Terms such as "SHSI" and "SBU" describe broad types of potentially sensitive information that might not even fall within any of the FOIA exemptions.

– DOJ Freedom of Information Act Guide[xvii]

FOIA Treatment	Policy / Agency
Ordinary review	FOUO / DHS FOUO / NRO LOU / DOJ OUO / NRC
No FOIA Release	SSI / TSA (3) SSI / DOT (3) PCII / FAA (3) PCII / DHS (3) SHSI / FAA (3) UCNI / DOD (3)
FOIA Exemptions, Applicable	CBI / EPA (4) ECI / EPA (7) FOUO / DOD (2-9) FOUO / FAA (2-9) OUO / DOE (2-9) PROPIN / NRC (4) SBU / State (2-9)
FOIA Exemptions, Suggested	CAI / EPA (2,5) SSI / USDA (2-4, 7) WMD / State (2, 4)
Ashcroft Memo	SHSI / NRC WMD / State WMD / Treas.
Specific Authorization	PCII / FAA SBU / CDC SBU / GSA SSI / TSA SSI / USDA
No policy / not available	DEA Sensitive Sensitive / DOD SGI / NRC Technical / DOD UCNI / DOE

The instances where a policy absolutely forbids release of certain unclassified information involve statutes that clearly proscribe disclosure under Exemption 3. For example, DHS regulation prohibits any release of **Protected Critical Infrastructure Information (PCII)**, a new designation created by the Homeland Security Act, Sec. 212: "**Protected CII** shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information."[28]

It is important to note several other approaches that agencies have taken in light of the conflict between their policies and the statutory language of FOIA. Some agencies require specific authorization on a case-by-case basis before controlled materials can be released under FOIA. This practice moves review of SBU-designated information one step beyond that ordinarily conducted under FOIA, such that FOIA managers who receive requests for this type of information must consult agency officials outside of their ordinary processing protocol. It is unclear whether these agencies have further specified detailed procedures for how such a review is to take place.

In some cases, as well, agencies have written their policies explicitly to comply with Attorney General Ashcroft's October 12, 2001 memorandum, or at least to abide by the general spirit of its mandate. In it, the Attorney General stated: "I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."[29] Several agencies, including the Departments of State and Treasury, have adopted the Card Memo's formulation of weapons of mass destruction (WMD) and other sensitive homeland security information as part of their information management program. Other policies reference the memo and/or demand more attentive review of specified information under certain exemptions with a view towards withholding, if at all possible.

In other cases, agency officials have provided employees with "suggested" FOIA exemptions, those under which the particular information in question *may* qualify for withholding. Potentially, this policy approach could make freedom of information personnel more likely to try to "find" an exemption for information that may not be precisely addressed. For example, USDA encourages its personnel to process requests "with consideration of all applicable FOIA exemptions" and lists four "FOIA Exemptions Potentially Applicable to SSI:

(1) For SSI pertaining to USDA operations or assets, FOIA Exemption 2 should be considered;
(2) For current SSI consisting of private sector or industry information submitted voluntarily to USDA that is customarily protected by the submitted, FOIA Exemption 4 should be considered;
(3) For any SSI the disclosure of which is banned by federal statute, FOIA Exemption 3 should be considered; and
(4) For any SSI that consists of information compiled for law enforcement purposes, FOIA Exemption 7 should be considered."

There are several different but equally significant problems with the treatment of designated sensitive unclassified information under the FOIA. The Executive Branch is already governed by an overarching policy regarding the protection of information that is unclassified but may nonetheless be inappropriate for public release, codified in FOIA Exemptions 2 through 9. In 1966, Congress expressly permitted agencies to shield from public view certain types of information, the nondisclosure of which respects a significant and identifiable government interest. Without necessitating amendment, Congress also left the door open for itself to expand the scope of FOIA, namely by passing a statute that would exempt particular information under Exemption 3, 5 U.S.C. § 552(b)(3), which safeguards information that is exempt under other laws.

The statutory FOIA language, however, nowhere sanctions internal agency decisions that would potentially override the FOIA in specific situations. Although none of the agency policies do this overtly, the prevalence of merged definitions, where information ordinarily protected under the FOIA is given the additional shield of a formal coversheet and an **SBU** or **FOUO** stamp, somehow suggests an additional level of security between it and the public. Logic dictates that information flagged and reviewed in FOIA offices before it is circulated to members of the public is already getting special treatment, and that an additional marking is superfluous; the same rationale would suggest that information designated as sensitive unclassified information must be different (i.e. *more* sensitive) than materials ordinarily controlled under FOIA. If nothing else, the psychological impact of supplementary control designations applied to unclassified information has the potential to reduce the amount of information that will now be released under FOIA.

AGENCY PROCESSING OF FOIA REQUESTS

PROCESSING TIME

For both the Card Memorandum and sensitive unclassified information FOIA requests, we assumed that the information necessary to respond would be easily identifiable by agency FOIA offices. None of the materials we received were classified or otherwise significantly protected, and many can be found on agency Internet sites. As such, the search from the perspective of FOIA officers should have been relatively simple in comparison to the numerous topic-specific or sensitive issue-related FOIA requests received in most offices. The policies at issue are themselves part of agency information management regimes, and so it would be logical for these policies and guidelines to be located within the FOIA office at each agency.

In fact, the processing of the FOIA requests varied enormously. The range of response times for the Card Memorandum request was 9-702 business days, and two requests are still pending over 750 business days later. The range for the sensitive unclassified information requests was 6-186 business days, and nine requests are still pending. In both cases there are still agencies that have not responded at all. These delays illustrate the limitations of using FOIA for informed public policy debate. While the passage of significant time, the persistence of researchers, and the responsiveness of certain FOIA officers has resulted in the release of useful records, this experience demonstrates that there are still significant backlogs in the current federal FOIA system.

It was clear from reviewing the materials provided by most agencies which office within the agency or organization is specifically responsible for the creation and/or oversight of the policy. In four cases, the responsible body was one tasked with information management or information security specifically (e.g., the Office of Information Resources Management at AID, the Personnel and Document Security Division at USDA, and Information and Physical Security at Treasury). In seven other cases, the task fell within a more general security office (such as NASA's Office of Security and Program Protection and NRC's Office of Nuclear Security and Incident Response). The rest of the policies came from another source, including general operations or a very high-level individual such as the secretary or administrator (the latter occurs in three agencies). The problems that some agencies had with processing the requests suggests that these security offices may not be adequately integrated with the records management and FOIA branches of the agencies.

DISPARITY IN RESPONSES

In addition, the type of information released varied significantly, with some agencies releasing extensive communications demonstrating their policy development and implementation activities and other agencies releasing only limited formal documentation of policies (which, in many cases, were publicly available). Thus, the subjectivity of release decisions can have a significant impact on the value of FOIA for informing the public about the activities and operations of government.

For example, a common problem was lack of understanding or misinterpretation of the FOIA requests. At some agencies (including State, DHS, and Energy), **FOUO** or **SBU information** can be designated by *any employee*, which assumedly includes those employees who process FOIA requests. However, we encountered several inquiries about the nature of the request itself. Furthermore, several agency representatives expressed a concern that our request was too broad, which questions the suitability of the searches conducted; for example, a search for "sensitive unclassified information" in a poorly organized records system might return those documents which are marked for protection per the agency policy in addition to documents establishing or discussing the policy. The Department of the Army denied any further processing of our request, declaring it too broad; however, a search of the Army's Web site produces Army Regulation 25-55, "The Department of the Army Freedom of Information Act Program," a chapter of which is entitled **"For Official Use Only."** These sorts of problems and inconsistencies cannot be addressed without adequate communication channels between FOIA requesters and FOIA offices, and educated FOIA officers with adequate records management training and adequate tools and resources.

In addition, several of the agencies that responded favorably released documents generally unrelated to the request or unhelpful in revealing the relevant policies of their agency, suggesting either a faulty search or the absence of relevant

documents. Two of these agencies–the Department of Veterans' Affairs and the Department of Housing and Urban Development–provided us with guidelines related to information security in the employment context, including criteria for background checks or security clearances and sensitivity designations for various positions at the agency that require access to sensitive or classified information.

In one case, the Department of State failed to provide us with the section of their Foreign Affairs Manual, 12 FAM 540, entitled **"Sensitive But Unclassified Information (SBU)"** but instead sent a different section of the same manual, 5 FAM 470, "Access to and Use of Information," which details general policies about employees' access to records, sharing of State Department records with other government agencies, and general release of agency records under the FOIA. The section that defines **SBU information** specifically and outlines procedures for its treatment is available on the State Department's Web site, and was provided to us by USAID, which also follows this policy.

RECOMMENDATIONS: STRATEGIES AND BEST PRACTICES TO SECURE AND SHARE SENSITIVE INFORMATION

Our research and appraisal of current agency practice shows a system that is seriously flawed. The diversity of policies, ambiguous or incomplete guidelines, lack of monitoring, and decentralized administration of information controls on unclassified information is troubling from the perspectives of safety, security, and democracy.

MONITORING OF PROTECTED DOCUMENTS

Arguably the most significant problem with agencies' protection of unclassified information is the lack of data concerning how many protected documents exist and the unavailability of any means to find out. The absence of reporting systems makes any assessment of the extent to which a policy is being used difficult, if not impossible. In written questions from the House Subcommittee on National Security, Emerging Threats, and International Relations, in conjunction with its recent hearing on pseudo-classification, Rear Admiral Christopher McMahon of the Department of Transportation, Office of Intelligence, Security, and Emergency Response, was asked how many FOUO, SSI, or similar designation decisions were made by DOT and its components. Admiral McMahon responded, "During the period in question, we did not keep records of restricted information designations other than national security classifications. Since January 2005, we have kept records of SSI designations, of which there have been two. Information has also been designated as 'For Official Use Only' this year, but we have no record of how many times."[30]

[V]ery little of the attention to detail that attends the security classification program is to be found in other information control marking activities. Key terms often lack definition. Vagueness exists regarding who is authorized to applying markings, for what reasons, and for how long. Uncertainty prevails concerning who is authorized to remove markings and for what reasons.
– Harold C. Relyea, Congressional Research Service[xviii]

In comparison, it is useful to look to the formal classification system, which is governed by Executive Order 12958, as amended, and is managed and monitored by the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA). ISOO publishes an annual report to the President in which they quantify the number of classification and declassification decisions, the number of individuals with authority to classify material, and the type of information that is being classified.[31] Such reports enable the Executive Branch and Congress to monitor the costs and benefits of the classification system and to identify trends that may suggest the need to reform the system.

Because safeguarding sensitive unclassified information impacts safety, security, budget and information disclosure–all important national concerns–some form of overarching monitoring of *all* information control would be valuable. Agencies should be required to maintain a record of who can use sensitive unclassified information designations and how many documents they designate for protection. Furthermore, the agencies should be required to maintain a record of how often FOIA officials release or withhold documents that have been marked as sensitive. Such data would make it possible for Congress and the public to be able to assess agency secrecy.

The Government Accountability Office (GAO) recently conducted a study of TSA's new Sensitive Security Information (SSI) policy at the request of members of Congress. GAO's report concluded that the omission of oversight mechanisms of any sort was a serious problem: "internal control policies and procedures for monitoring the compliance with regulations governing the SSI designation process, including internal controls for ongoing monitoring, communicated to all staff, would help ensure accountability and consistency in the implementation of TSA's SSI regulations."[32]

THE BLACK HOLE OF INFORMATION SAFEGUARDING

The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-related information for which there is no usable definition, no common understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection.
- Heritage Foundation Special Report (2004) [xix]

For classified information, the security classification system provides precise limits on the extent and duration of classification as well as a system for declassification, including public requests for declassification. For non-security sensitive information, the FOIA provides a relatively clear and user-friendly process for the public to seek access to information held by the government. Sensitive unclassified information, however, falls into a black hole. As this Study shows, it is likely that information previously available under FOIA or on unrestricted Web sites may no longer be available to the public. Yet, there is virtually no opportunity for the public or other government personnel to challenge a decision to mark a document for protection as **SBU**, **FOUO**, or **SSI**. Accordingly, in order to protect the important role that public access has played in government accountability, it is important that a system for challenging the use of sensitive unclassified information markings be established at each agency or, alternatively, that FOIA procedures be adjusted to counteract the chilling effect that these markings may have on disclosure under FOIA. Moreover, classified information is subject to limits on the duration of protection, but few such limits exist for SUI. Thus, once marked may mean forever marked.

THE HIDDEN COSTS

ISOO reports annually on the estimated costs of classification and declassification activities throughout the government. During FY 2004, agencies spent a total of $4.3 billion on information security generally, including classification and declassification management and security for information systems; an additional $691 million was spent on physical security for buildings and storage of classified information.[33] By referring to the chart on page 19, which depicts the range of safeguarding methods that are applied to unclassified information by some agencies, it is apparent that many of the measures mirror those applied to classified information. It is possible, therefore that some portion of the spending ISOO reported was in fact used for unclassified information protection. Convenience, resource constraints, or established practices may lead to the commingling of classified and sensitive unclassified materials in order to ensure both are properly safeguarded. If this occurs, it could potentially undermine the security of the classification system. Accordingly, agencies should be required to take steps to assess the cost of their sensitive unclassified information systems and ensure that safeguards do not undermine the security of classified information.

Moreover, the cost of an impaired information sharing system cannot by quantified. There are two aspects to this problem. The first, which has been well-documented, is the problem of inter-agency information sharing. The second is the problem of public-private sector information sharing; if private industry is unable to learn information and is required to adopt restrictions on information from the government, it may be well inhibit the willingness of private industry to engage in activities that could benefit the public good.

A UNIFIED SYSTEM

This Study suggests that a great deal of non-sensitive information is being withheld today that should be or previously would have been released under the FOIA. It is also likely, however, that the current system of diverse and unregulated safeguard mechanisms is not actually succeeding in shielding much of the information that could be useful to terrorists or others desiring to undermine the security of the United States. Even Secretary of Defense Rumsfeld has recognized that **FOUO** is not working properly at the Department of Defense,[34] and similar policies are probably not achieving their goals elsewhere across the federal government.

An Al Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." At more than 700 gigabytes, the DOD web-based data makes a vast, readily available source of information on DOD plans, programs, and activities. One must conclude our enemies access DOD web sites on a regular basis. . . . The fact that for official use only (FOUO) and other sensitive unclassified information (e.g. CONOPS, OPLANS, SOP) continues to be found on public web sites indicates that too often data posted are insufficiently reviewed for sensitivity and/or inadequately protected. Over 1500 discrepancies were found during the past year. This continuing trend must be reversed.
– Sec. of Defense Donald Rumsfeld[xx]

Although classification is centrally managed, agencies implement their own classification programs according to central guidance and criteria, in a way that makes sense within the function and mission of their particular organization. ISOO Director J. William Leonard has recommended that a unified framework be instituted to both simplify and supervise control of unclassified information as well. In his proposed structure, Leonard offers several suggestions that seem appropriate, particularly in light of our findings. He advocates for: "Strict limitations as to who can designate information as falling under the system of controls"; "Built-in criteria that must be satisfied in order to place controls on dissemination"; "Uniform 'due-diligence' standards with respect to how to handle and protect controlled information"; and "A process . . . whereby both authorized holders and outsiders can appeal the application of dissemination controls."[35]

This Study suggests that issues of information security, information sharing, and public access to information should not be addressed in a piecemeal manner. There are best practices in agencies that should be shared, as well as lessons to be learned about the costs and benefits of secrecy and disclosure. Unnecessary secrecy has been on the rise since September 11, with the result of threatening our safety and national security while impeding the process of democracy and the effective functioning of the government. In presenting markers of possible successes and failures of sensitive unclassified information programs among the federal agencies, this Study seeks to offer a rationale and a sense of urgency for initiating reforms, in these and other information-control programs government-wide.

ENDNOTES

[1] William J. Broad, "A Nation Challenged; The Biological Threat; U.S. Is Still Selling Reports on Making Biological Weapons," The New York Times, at A1 (Jan. 13, 2002).
[2] *See, e.g. Emerging Threats: Overclassification and Pseudo-Classification,* Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005).
[3] *Government Information Policies and Practices–Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, Hearing before the Foreign Operations and Government Information Subcommittee of the U.S. House Committee on Government Operations, 92nd Cong. (1972) (Opening statement of Chairman Moorhead), at 2283.
[4] *Id* (questioning by William G. Phillips, Staff Director), at p. 2498.
[5] President Jimmy Carter, "Telecommunications Protection Policy," PD/NSC-24 (Nov. 16, 1977)
[6] For more background, see Genevieve Knezo, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, Congressional Research Service, RL 31845 (July 2, 2003).
[7] The Computer Security Act of 1987, 40 U.S.C. 1441 (1987).
[8] *Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997) [hereinafter "Moynihan Commission Report"], http://www.access.gpo.gov/congress/commissions/secrecy/.
[9] Homeland Security Act of 2002, 6 U.S.C. § 482(a).
[10] The Archive faxed a FOIA request to the Office of Management and Budget (OMB) on January 9, 2003.
[11] Defense Information Systems Agency, "DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements," Version 1.2, Attachment 5 (Mar. 19, 1999).
[12] *Id.* at 6-7.
[13] *Id.* at 9.
[14] *Id.* at 12.
[15] http://www.openthegovernment.org/otg/SRC2005.pdf.
[16] Department of Justice, *FOIA Post: Critical Infrastructure Information Regulations Issued by DHS* (2004), http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm.

[17] Homeland Security Act of 2002, 6 U.S.C.A. § 482(f)(1).
[18] Homeland Security Act of 2002, 6 U.S.C.A. § 482(c).
[19] Because several of the responsive agencies have multiple policies to protect different categories of sensitive information, and because a number of agencies have no reported policy, the number of different SBU-like policies to be analyzed is different from the number of agencies considered. In addition, some agencies share policies–for example, a DHS-wide directive on SBU information applies at least in name to each component of the department, and AID follows the SBU policy set forth by the Department of State in its *Foreign Affairs Manual*. Please note, however, that this study has not combined policies with the same title or similar definition, where those policies are distinct in that they have been internally or otherwise derived from different sources or are substantially different in any other way.
[20] U.S. Government Accountability Office, "Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information," GAO-05-677 Report to Congressional Requesters (June 2005), at 3.
[21] Remarks of J. William Leonard, Director, Information Security Oversight Office (ISOO), at the National Classification Management Society's Annual Training Seminar, Salt Lake City, UT (June 12, 2003).
[22] *Conference Report on H.R. 2360, Department of Homeland Security Appropriations Act*, H.R. Conf. Rep. No., at 109-241 (2006).
[23] Spencer S. Hsu, *Homeland Security Employees Required to Sign Secrecy Pledge; Gag Order Raises Concern on Hill*, Washington Post (Nov. 16, 2004).
[24] John Files, *Security Dept. Eases Its Nondisclosure Rule*, New York Times (Jan. 18, 2005).
[25] Homeland Security Act Sec. 892(c)(2). The President delegated authority to regulate in accordance with the Act in Executive Order 13311, in July 2003.
[26] U.S. National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (Washington: GPO, 2004), at 417-18.
[27] Moynihan Commission Report, *supra* note 8.
[28] Disclosure of Protected Critical Infrastructure Information, 6 C.F.R. §29.8; *see also* Homeland Security Act of 2002 § 214, 6 U.S.C.A. § 133(a)(1).
[29] Memorandum for Heads of All Federal Departments and Agencies: "The Freedom of Information Act," from Attorney General John Ashcroft (October 12, 2001), http://www.usdoj.gov/04foia/011012.htm.
[30] McMahon letter to Representative Christopher Shays, Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, U.S. House of Representatives (May 9, 2005).
[31] *See, e.g.*, Information Security Oversight Office (ISOO), "Report to the President 2004" (March 31, 2005), http://www.archives.gov/isoo/reports/2004-annual-report.html.
[32] GAO, *supra* note 20, at 7.
[33] ISOO, *2003 Report on Cost Estimates for Security Classification Activities* (July 2004), http://www.archives.gov/isoo/reports/2003-cost-report.html.
[34] Sec. of Defense Donald Rumsfeld, Cable: "Web site OPSEC discrepancies," January 14, 2003, http://www.fas.org/sgp/news/2003/01/dodweb.html.
[35] Leonard remarks, *supra* note 21.

QUOTATIONS

[i] Remarks of J. William Leonard, Director, Information Security Oversight Office (ISOO), at the National Classification Management Society's Annual Training Seminar, Salt Lake City, UT (June 12, 2003).
[ii] *Executive Classification of Information, Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act*, U.S. House of Representatives, Committee on Government Operations, H.R. Rep. 93-221 (1973).
[iii] Report of the Commission on Protecting and Reducing Government Secrecy ("Moynihan Commission Report"), Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997), http://www.access.gpo.gov/congress/commissions/secrecy/
[iv] Coalition of Journalists for Open Government, Comments on Proposed Regulations: In the Matter of Protection of Sensitive Security Information (filed July 16, 2004), http://www.cjog.net/protest_sensitive_security_inform.html.
[v] *Emerging Threats: Overclassification and Pseudo-Classification,* Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005) (Statement of Representative Christopher Shays, Chairman), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:20922.wais.
[vi] U.S. Department of Justice, *Freedom of Information Act Guide* (May 2004), http://www.usdoj.gov/oip/foi-act.htm.
[vii] Sec. of Defense Donald Rumsfeld, Cable: "Web site OPSEC discrepancies," January 14, 2003, http://www.fas.org/sgp/news/2003/01/dodweb.html.
[viii] Emerging Threats: Overclassification and Pseudo-Classification, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005) (Statement of Harold C. Relyea, Congressional Research Service).

[ix] *Government Information Policies and Practices–Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, Hearing before the Foreign Operations and Government Information Subcommittee of the U.S. House Committee on Government Operations, 92nd Cong. (1972) (Opening statement of Chairman Moorhead), at 2283.

[x] President Dwight D. Eisenhower, Farewell Radio and Television Address to the American People (January 17, 1961).

[xi] Remarks of J. William Leonard (2003).

[xii] *Id*.

[xiii] MITRE Corporation, JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance* (Dec. 2004), p. 5, *available at* http://www.fas.org/irp/agency/dod/jason/classpol.pdf.

[xiv] Coalition of Journalists for Open Government, Comments on Proposed Regulations: In the Matter of Protection of Sensitive Security Information (filed July 16, 2004), http://www.cjog.net/protest_sensitive_security_inform.html.

[xv] Statement of Representative Christopher Shays (2005)

[xvi] Moynihan Commission Report (1997).

[xvii] DOJ, *FOIA Guide* (2004).

[xviii] Statement of Harold C. Relyea (2005).

[xix] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report* (Dec. 13, 2004), p. 27, http://www.heritage.org/Research/HomelandDefense/sr02.cfm.

[xx] Rumsfeld Cable (2003).

FURTHER READING

Aftergood, Steven & Henry Kelly, "Making Sense of Information Restrictions After September 11," 55 *Federation of American Scientists Public Interest Report* 2 (March/April 2002).

Bagley, James J., "Understanding Controls on Unclassified Government Information or 'Who's on First?'" National Classification Management Society, NCMS Viewpoints (1993), http://www.fas.org/sgp/eprint/bagley.html.

Buchalter, Alice R. et al., "Laws and Regulations Governing the Protection of Sensitive But Unclassified Information," Federal Research Division, Library of Congress (Sept. 2004).

Emerging Threats: Overclassification and Pseudo-Classification, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:20922.wais.

Executive Classification of Information–Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act, H.R. Rep. No. 93-221 (1973).

Government Information Policies and Practices–Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7), Hearing before the Subcomm. Foreign Operations and Government Information of the H. Comm. on Government Operations, 92nd Cong. (1972).

Knezo, Genevieve J., "'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy," CRS Report RL31845 (July 2, 2003).

OMB Watch, *Background on Sensitive But Unclassified Information* (2005), http://www.ombwatch.org/article/archive/238?TopicID=2.

OpenTheGovernment.org, "Secrecy Report Card 2005" (Sept. 4, 2005), http://www.openthegovernment.org/otg/SRC2005.pdf.

Report of the Commission on Protecting and Reducing Government Secrecy, Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997), http://www.access.gpo.gov/congress/commissions/secrecy/.

Reporters Committee for Freedom of the Press, "Homefront Confidential" (June 8, 2005).

Sollenberger, Mitchel A., *Sensitive Security Information and Transportation Security: Issues and Congressional Options*, Congressional Research Service RL32425 (June 9, 2004).

Sollenberger, Mitchel A., *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, Congressional Research Service RS21727 (Feb. 5, 2005).

U.S. Department of Justice, "Critical Infrastructure Information Regulations Issued by DHS," *FOIA Post* (Feb. 27, 2004), http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm.

U.S. Government Accountability Office, "Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information," GAO-05-677 Report to Congressional Requesters (June 2005).

U.S. House of Representatives, Committee on Government Reform, Minority Staff, "Secrecy in the Bush Administration," Report prepared for Rep. Henry A. Waxman (Sept. 14, 2004), http://democrats.reform.house.gov/features/secrecy_report/pdf/pdf_secrecy_report.pdf.

APPENDIX I
CARD MEMORANDUM FOIA REQUESTS, BY PROCESSING TIMES
SUMMARY OF AGENCY PROCESSING

Number of Business Days	Agency	Number of Documents / Pages Provided
9	Federal Bureau of Investigation	No Documents
11	Health and Human Services	No Documents
12	National Science Foundation	1 Document (1 p.)
16	Dept of Housing and Urban Development	No documents
24	Department of Education	No Documents
24	Environmental Protection Agency	3 Documents (18 pp.), 107 Documents withheld **Appeal Pending**
26	Department of Navy	1 Document (7 pp.)
27	General Services Administration	2 Documents (3 pp.)
30	Small Business Administration	2 Documents (2 pp.)
31	Federal Emergency Management Agency	1 Document (1 p.)
32	Department of Interior	13 Documents (81 pp.), 7 Documents withheld
34	Department of Commerce	13 Documents (25 pp.), 16 Documents withheld
35	Department of Treasury	15 Documents (27 pp.)
36	Office of Management & Business	No Documents
41	Department of Labor	3 Documents (3 pp.)
41	Department of Veterans Affairs	2 Documents (2 pp.)
42	Department of Justice	5 Documents (14 pp.), 40 Documents withheld
46	Department of Agriculture	2 Documents (10 pp.)
61	Drug Enforcement Agency	1 Documents (3 pp.)
69	Nuclear Regulatory Commission	16 Documents (32 pp.)
94	Office of Personnel Management	No Documents
103	Department of Defense	86 Documents (125 pp.)
103	National Archives and Records Admin.	3 Documents (6 pp.)
104	Department of Army	3 Documents (7 pp.)
110	Department of Air Force	9 Documents (63 pp.)
118	Department of Energy	63 Documents (152 pp.)
137	Social Security Administration	1 Document (10 pp.)
151	Defense Intelligence Agency	No Documents
151	Department of Transportation	78 Documents (150 pp.)
160	Securities and Exchange Commission	No Documents
197	U.S. Central Command (CENTCOM)	No Documents
217	Department of State	4 Documents (11 pp.)
* 702	National Aeronautics and Space Admin.	1 Document (2 pp.)
750+	U.S. Agency for International Development	**Request Pending**
750+	Central Intelligence Agency	**Request Pending**

***** On October 25, 2002 NASA provided responsive documents, including its reply to the White House regarding the Card Memo, in response to a previous request from the National Security Archive for documents on Attorney General John Ashcroft's October 12, 2001 memo on FOIA policy.

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
AID	**No Response**	**No Response**	**No Response**	**No Response**	**No Response**	**No Response**
AIR	YES, *see* DOD regarding joint response	YES	YES	Web information removal; review of records	Additional review for CBRN[ii]	New Security Training
ARMY	YES, *see* DOD regarding joint response	YES	YES	Web information removal; review of records	Additional review for CBRN	Dissemination of Card Policy
CENTCOM[iii]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
CIA	**No Response**	**No Response**	**No Response**	**No Response**	**No Response**	**No Response**
DEA[iv]	No Documents[v]	No Documents	No Documents	No Documents	No Documents	No Documents
DIA[vi]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
USDA	YES	YES		Inventoried Web sites; new review procedures	Guidance to use FOIA Exemptions 2, 3 and 7 for sensitive security information	New personnel security and information security measures; new departmental regulations; sought classification authority
DOC	YES	YES	YES			Dissemination of Card guidance
DOD	YES, Joint Military Response	YES	YES	Web information removal; review of records	Additional review for CBRN	New classification guide; new procedures for sharing unclassified sensitive information
DOE	YES	YES	YES	Web information removal; New Security Measures	Additional Review Of Requested Records; New Guides For FOIA Exemptions	New Information Security Guides; Dissemination of Card guidance
DOI	YES	YES	YES	Web information removal	Special Handling of FOIA Requests; dissemination of Card guidance to FOIA officers	Dissemination of Card guidance
DOJ					FOIA Exemption Guidance Disseminated; training on FOIA exemptions 1, 2,3, 4.	Guidance and policies concerning Classified, Declassified and SBU information disseminated.
DOL	YES	YES	YES	Web review (possible info removal); updated Web policies	Guidance on withholding under FOIA	Dissemination of Card guidance
DOS					FOIA Exemption 2 and 4 Guidance Disseminated; training on guidance	Guidance and policies concerning safeguarding information disseminated
DOT	YES	YES	YES	Web information removal; new Web procedures	New Procedures for FOIA Review	New security policies
EDU	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
EPA	YES	YES	YES	Web information removal; new procedures	Emphasis on FOIA Exemptions 2 and 4	Dissemination of Card guidance
FBI[vii]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
FEMA	YES	YES	YES			
GSA	Yes	YES	YES		Review of FOIA Policies	Non Disclosure Agreements; new safeguarding procedures
HHS	No Documents	No Documents	No Documents	No Documents	Card Memo Disseminated to FOIA Offices[viii]	No Documents
HUD	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
NARA	No Documents[ix]	No Documents	No Documents	No Documents	No Documents	No Documents
NASA[x]	No Response	YES	YES	Web sites Blocked; New Web procedures	Card Memo disseminated to FOIA Offices	Dissemination of Card guidance; New Security Program
NRC	YES	YES	YES		Guidance For Withholding Information Under FOIA	
NSF	YES	YES	YES			
OMB	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
OPM	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
SBA	YES	YES	YES			Dissemination of Security Information
SEC	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
SSA	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
TRE	YES	YES	YES			Dissemination of Card guidance
USN (NAVY)	YES, see DOD regarding joint response	YES	YES		Disseminated to FOIA Offices; Refers to Ashcroft Memorandum for FOIA Exemptions	

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
VET	YES	YES	YES			Dissemination of Card guidance

[i] Agencies that did not respond are listed in bold.
[ii] CBRN means Chemical Biological Radiological and Nuclear information.
[iii] CENTCOM is a component of DOD.
[iv] DEA is a component of DOJ.
[v] DEA provided copies of the Card Memorandum and ISOO-OIP Guidance.
[vi] DIA is a component of DOD.
[vii] FBI is a component of DOJ.
[viii] Although HHS reported no documents, a later correspondence indicated that the Card Memorandum was disseminated to FOIA offices.
[ix] NARA withheld records concerning the ISOO-OIP Guidance and offered to send the Card Memorandum and the ISOO-OIP Guidance.
[x] NASA did not respond to the Card FOIA request, but this information was obtained from a NASA response to an earlier FOIA request filed by the Archive for information concerning the implementation of the Ashcroft Memorandum. (See http://www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB84/index.html)

APPENDIX III
SENSITIVE UNLASSIFIED INFORMATION FOIA REQUESTS, BY PROCESSING TIME

Number of Business Days	Agency	Number of documents / Pages provided
6	National Science Foundation	1 Document (2 pp)
14	Social Security Administration	No Documents
14	Treasury Department	8 Documents (51 pp)
16	Small Business Administration	No Documents
19	Department of State	3 Documents (12 pp)
20	Department of Agriculture	3 Documents (18 pp)
21	Federal Aviation Administration	2 Documents (19 pp)
25	Securities and Exchange Commission	No Documents **Appeal Pending – new search in progress**
26	Office of Management and Budget	No Documents
27 IG 29 Citizen Services	General Services Administration	1 Document (3 pp) – IG 2 Documents (13 pp) – Citizen Services
40	Environmental Protection Agency	1 Document (66 pp)
41	Department of Justice, OIP	No Documents – forwarded to DHS
42	Veterans' Administration	3 Documents (54 pp)
43	Federal Emergency Management Agency	No Documents – forwarded to DHS
43	Transportation Safety Administration	3 Documents (45 pp)
45	National Aeronautics and Space Agency	4 Documents (210 pp)
49	Housing and Urban Development	1 Document (22 pp)
55	Office of Personnel Management	No Documents
71	National Reconnaissance Office	5 Documents (43 pp)
105	Department of the Air Force	No Documents, list of publicly available docs
112	Nuclear Regulatory Commission	20 Documents (223 pp), list of publicly available documents
113	National Institutes of Health	No Documents, refer to HHS request
144	Department of Commerce	No Documents
146	US Agency for International Development	36 Documents (185 pp)
152	Department of Homeland Security	6 Documents (81 pp)
169	Drug Enforcement Agency	1 Document (29 pp)
68 Mgmt. Division 171 Criminal Division	Department of Justice	2 Documents (281 pp) 3 Documents (26 pp)
176	Department of Transportation	59 Documents (382 pp), 99 withheld
250	National Geospatial-Intelligence Agency	3 Documents (81 pp)
* 11	National Archives and Records Administration	No Documents
* 23	Department of the Army	Request denied, too broad Follow-up pending, Army General Counsel
* 26	Department of Energy	12 Documents (177 pp)
42 *** 186 – new request**	**Federal Bureau of Investigation**	2 Documents (6243 pp) - request too broad **Request denied – no documents** **Appeal pending**
*** 140**	**Centers for Disease Control**	**Request pending** (not yet acknowledged)
*** 160**	**Customs and Border Protection**	**Request pending** (not yet acknowledged)
*** 260+**	**Central Intelligence Agency**	**Request pending** (acknowledged 3/29/05)
*** 260+**	**Citizenship and Immigration Service**	**Request pending** (acknowledged 2/28/05)
*** 260+**	**Defense Intelligence Agency**	**Request pending** (acknowledged 3/17/05)
*** 260+**	**Department of Defense**	**Request pending** (acknowledged 3/9/05)
*** 260+**	**Department of Interior**	**Request pending** (acknowledged 2/28/05)
*** 260+**	**Department of Health and Human Services**	**Request pending** (acknowledged 2/28/05)
*** 260+**	**Immigration and Customs Enforcement**	**Request pending** (acknowledged 6/8/05)

***** All figures shown with ***** are dates and figures that differ from the standard methodology.

APPENDIX III
SENSITIVE UNLASSIFIED INFORMATION FOIA REQUESTS, BY PROCESSING TIME

DOE reported no record of receiving original request in 2/05, and therefore did not begin processing until a later date; this request was resent on 6/6/05. The initial request sent in 2/05 were sent to confirmed agency fax numbers and received a positive receipt of transaction, however for unknown reasons were never entered into the agency's tracking systems.

NARA – agency final response letter was dated 3/14/05, but was never received by the Archive; after an inquiry, the response was resent on 9/19/05.

CBP request was resent on 7/18/2005 (originally sent to wrong office but was not forwarded; after inquiry, the Archive resent the request to Office of Regulations and Rulings).

CDC request was sent as an addition to the Audit, on 8/15/2005, based on information learned during our research for this report; the chart reflects the current time of processing since that request was sent.

FBI initial response advised that the request was too broad and suggested the Archive review the FBI Manual of Operations and Procedures and the Manual of Investigative Operations and Guidelines. On 6/9/05, the Archive filed a new, more specific request based on these manuals. The second request was subsequently denied as too broad; follow-up inquiries are pending.

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
AID	Sensitive But Unclassified (SBU)	Internal 12 Foreign Affairs Manual (FAM) 540 [updated 4/25/02]	Broad categories, examples	Supervisory employee	No policy	Need-to-know AND background check	Moderate	Info exempt under FOIA = SBU Review case-by-case
AIR **	For Official Use Only (FOUO)	Internal DOD Dir. 5400.7-R 9/1/1998	FOIA Exemptions	Any employee	Originator OR designated official	Need-to-know AND government business	Moderate	Review
AIR **	Sensitive Information (Computer Security Act, 1987)	Statutory PL 100-235 [DOD 8500.1]	Broad definition	N/A	N/A	Need-to-know	N/A	Review
ARMY*	For Official Use Only (FOUO)	Internal Army Reg. 25-55 11/1/1997 Army Reg. 380-19 3/27/1998	FOIA Exemptions	Any employee	Originator OR other authority (FOIA reviewer)	Need-to-know AND government business	High – transmission	Review
CBP* †	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
CDC* †	Sensitive But Unclassified (SBU)	Internal CDC-02 Manual 7/22/2005	Categories Examples	Designated officials	Same	Need-to-know	Moderate	Review, authorization Suggested exemptions
CIA †								
CIS* †	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
DEA	DEA Sensitive	Internal Reference Booklet 8/2002	Broad definition categories	Senior officials	N/A	Need-to-know	High	LOU may be exempt from release under FOIA
DHS	Protected Critical Infrastructure Information (PCII)	Statutory 6 U.S.C. 131(3), Homeland Security Act 6 CFR 29	Broad categories Administrative requirements	PCII Program Office	No policy	Specified activities; Training; explicit authorization; AND non-disclosure agreement	Moderate	Specific authorization OR Exemption 3

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
DHS	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [5/04, updated 1/6/05]	Broad categories with examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
DIA †								
DOA	Sensitive security information (SSI)	Internal, DR 3440-2 1/30/2003	Broad definition Categories Restriction on abuse	Senior officials [Head of Dept Org.]	Same	Need-to-know	Moderate	OGC authorization for release Ashcroft / Ex. 2, 4, 3, 7
DOC	No documents							
DOD* †	DoD Unclassified Controlled Nuclear Information (DOD UCNI)	Statutory 10 USC 128 DOD Dir. 5210.83 [11/15/1991]	Specific categories, guidance	Senior officials	N/A	Need-to-know AND U.S. citizen or government employee	Moderate	No disclosure under Exemption 3
DOD* †	For Official Use Only (FOUO)	Internal DOD Dir. 5400.7-R 9/1/1998	FOIA Exemptions	Any employee	Originator OR designated official	Need-to-know AND government business	Moderate	Review
DOD* †	Sensitive Information (Computer Security Act of 1987)	Statutory PL 100-235 [DOD 8500.1]	Broad definition	N/A	N/A	Need-to-know	N/A	Review
DOE	Unclassified Controlled Nuclear Information (UCNI)	Statutory 42 USC 2168, 10 CFR 1017.11 DOE Order 471.1A [update 6/30/00]	Categories, specific	Designated – Reviewing Officials	Same	Need-to-know	Moderate	Review
DOE	Official Use Only (OUO)	Internal DOE O 471.3 [4/903]	Broad definition Official guidance OR FOIA exemptions	Any employee	Guidance: any employee FOIA: originator	Need-to-know	Moderate	Review
DOI †								
DOJ	Limited Official Use (LOU)	Internal DOJ 2620.7 [9/1/1982, update 5/5/2005]	Broad definition, categories Limitation on abuse	Senior officials / designees	N/A	Need-to-know	Low	Review

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
DOJ/ OIP	Request forwarded to DHS							
DOS	WMD / Other Sensitive Homeland Security Info	Internal, 4/4/02 Based on Card Memo	Definition, categories	Originator	No policy	Need-to-know	Moderate	Review Ashcroft Memo: exemptions 2, 4
DOS **	Sensitive But Unclassified (SBU)	Internal 12 Foreign Affairs Manual (FAM) 540 [updated 4/25/02]	Broad categories, examples	Originator	FOIA reviewer	Need-to-know AND Background check	Moderate	Info exempt under FOIA = SBU Review
DOT	Sensitive Security Information (SSI)	Statutory 49 CFR Part 15	Specified categories	Designated senior officials	Secretary, in writing	Need-to-know	Moderate	Exemption 3 GC authorization
EPA	Confidential Agency Information (CAI)	Internal *Information Sensitivity Compendium*, 7/02	Broad definition Categories/ examples	Originator or info. manager	No policy	Need-to-know	Moderate/ high	Review (maybe exemption 2, 5)
EPA	Confidential Business Information (CBI)	Internal *Information Sensitivity Compendium*, 7/02	Definition, Categories (FOIA)	Originator or info. manager	No policy	Need-to-know	Moderate/ high	Exemption 4
EPA	Enforcement-Confidential Information (ECI)	Internal *Information Sensitivity Compendium*, 7/02	Definition, Categories (FOIA)	Originator or info. manager	No policy	Need-to-know	Moderate	Exemption 7
FAA	For Official Use Only (FOUO)	Internal	Definition / FOIA	Senior officials	Originator	Need-to-know	Moderate	Review
FAA	Sensitive Security Information (SSI)	Statutory 49 CFR Part 15	Categories	Secretary [categories] Senior Officials	No policy	Need-to-know	Moderate	No release, Ex. 3
FBI †								
FEMA								
GSA	Sensitive But Unclassified (SBU) Building Information	Internal Public Building Service (PBS) Policy, 3/8/02	Categories, examples	N/A	N/A	Need-to-know	Moderate	Authorization Ashcroft memo
HHS †								

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
HUD	No applicable documents							
ICE* †	**Sensitive But Unclassified [For Official Use Only] Information**	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
NARA	No documents							
NASA	**Administratively Controlled Information (ACI)**	Internal [11/3/04]	Categories	Senior officials	Originator	Need-to-know	N/A	No disclosure unless clearly in accordance with law – FOIA Review
NAVY †								
NGA	**For Official Use Only (FOUO)**	Internal [6/2004], references DOD Directive 5200.1	FOIA Exemptions	Any employee	N/A	Need-to-know AND government business	Moderate	Review
NIH	No documents							
NRC	**Safeguards Information (SGI)**	Statutory Atomic Energy Act 10 CFR 73	Categories with examples	Senior officials or Designated officials	Originator	Need-to-know AND Background check	High	Review
NRC	**Official Use Only (OUO)**	Internal [12/20/99]	Categories / FOIA	Senior officials (branch chiefs) OR Contractor designee	Originator or originator's supervisor	Need-to-know	Moderate	Review
NRC	**Proprietary Information (PROPIN)**	Internal [12/20/99]	Categories / FOIA Ex. 4	Senior officials (branch chiefs) OR Contractor designee	Originator	Need-to-know	Moderate	Review / no release under exemption 4
NRC	**Sensitive Homeland Security Information (SHSI)**	Internal [4/4/02] Complies with DHS proposed regulations	Categories Examples	Designated staff	N/A	Need-to-know	N/A	Review per Ashcroft memo, exemptions 2, 4
NRO	**For Official Use Only (FOUO)**	Internal [updated 4/14/03]	Categories / FOIA	Any employee	N/A	Need-to-know	Moderate	Review

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
NSF	Sensitive Information	Internal Memo 5/11/2000	N/A	Any employee	FOIA officer	Need-to-know	N/A	Review
OMB	No documents							
OPM	No documents							
SBA	No documents							
SEC	No documents							
SSA	No documents							
TRE	Sensitive But Unclassified Information (SBU)	Internal Directive [Card Memo, 4/4/02]	Card Memo	N/A	N/A	Need-to-know	Moderate	Review per Ashcroft Memo, Ex. 2, 4
TSA	Sensitive security info (SSI)	Statutory 49 CFR 1520.5	Categories 1520.7(a)-(r)	Any employee (info in given categories) OR Administrator (other info)	No policy	Need-to-know AND Non-disclosure agreement	Moderate	Review [FOIA officer and SSI Program Office]
TSA	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
TSA	Critical Infrastructure Information (CII)	Statutory 6 U.S.C. 131(3), Homeland Security Act						
VET	No applicable documents							

CHART KEY

Policy: Name/acronym for agency's policy regarding unclassified information that is otherwise protected

Authority: Statutory/regulatory or internal authority establishing or updating the policy

Guidance: Definition and/or other guidance to be followed by individuals in designating information under the policy

Designation: Individual(s) responsible for designating protected information within the agency

Removal: Individual(s) responsible for removing the designation of protected information

- Same: the same individual(s) who are allowed to designate protection are able to remove such protection
- Originator: only the specific individual (and in most cases the individual's supervisor(s) or successor) who made the original designation may remove it

Access: Qualification(s) for individuals who are authorized to access information protected under the policy

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

Protection: Degree of protection generally applied to documents/electronic media containing information designated under the policy
FOIA: Specific guidelines for treatment of FOIA requests for information protected under the policy

N/A: Not available
No policy: Based on the information collected, the agency's policy includes no specific guidance on this matter

† The Archive's FOIA request is still pending with this Agency (see processing chart, Appendix III)
* The information given was not provided by the Agency, but rather is based on our own research or materials submitted by other agencies.
** This Agency provided some information, but none regarding this specific aspect of their policy; the noted information is based on research or inference from other given information.

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
ACI / Administratively Controlled Information	NASA	11/3/2004	Internal NPR 1600.1	Categories (9)	Originating management official	Originator	Need-to-know	N/A	No disclosure except legal obligation (FOIA)
CAI / Confidential Agency Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with examples	Originator OR Information manager	No policy	Need-to-know	Moderate / High	Review / exemption 2 or 5
CBI / Confidential Business Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with Examples	Originator OR Information manager	No policy	Need-to-know	Moderate / High	Exemption 4
Computer Security Act Sensitive Information	DOD*	1/9/1988	Statutory PL 100-235 [DOD 8500.1]	Broad definition Categories	N/A	N/A	Need-to-know	Low	Review
DEA Sensitive	DEA DOD*	8/2002	Internal Reference Booklet	Broad definition categories, law enforcement-related	Senior officials	N/A	Need-to-know	High	LOU may be exempt from release under FOIA
ECI / Enforcement-Confidential Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with examples	Originator OR Information manager	No policy	Need-to-know	Moderate	Exemption 7
FOUO / For Official Use Only [DHS]	TSA DHS CBP* CIS* ICE*	5/2004 Update 1/6/2005	Internal DHS Directive 11042.1	Broad definition Categories with examples	Any employee	Originator OR Senior official	Need-to-know	Moderate	Review
FOUO / For Official Use Only [DOD]	DOD* AIR ARM* USN* NGA	9/1/1998	Internal DOD 5400.7-R	Categories (FOIA exemptions)	Any employee	Originator / designated officials	Need-to-know/ gov't business	Moderate	Review
FOUO / For Official Use Only [FAA]	FAA	6/13/2000	Internal FAA O 1270.1	Broad definition (based on FOIA)	Senior officials	Originator	Need-to-know	Moderate	Review

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
FOUO / For Official Use Only [NRO]	NRO	10/5/1999 Update 1/31/2003	Internal NROD 50-12	Categories (FOIA exemptions)	Any employee	Originator (with senior authorization)	Need-to-know	Moderate	Review
LOU / Limited Official Use Information	DOJ	9/1/1982 Update 5/5/2005	Internal DOJ O 2620.7	Definition Categories Examples	Senior official OR other designated	N/A	Balancing test	Low	Review
OUO / Official Use Only [DOE]	DOE	4/9/2003	Internal DOE O 471.3	Broad definition with specific guidance OR FOIA exemption	Any employee	Originator OR supervisor, FOIA official	Need-to-know	Moderate	Review
OUO / Official Use Only [NRC]	NRC	6/2/1998 Update 12/20/1999	Internal MD 12.6	Categories (FOIA exemptions)	Senior officials, selected	Originator OR supervisor	Need-to-know	Moderate	Review
PCCI / Protected Critical Infrastructure Info	DHS	2002	Statutory 6 USC 131 6 CFR 29	Specific definition Categories	Designated official	Same	Need-to-know	Moderate	Authorization / Exemption 3
PROPIN / Proprietary Info	NRC	12/20/1999	Internal MD 12.6	Categories (FOIA Exemption 4)	N/A	Originator	N/A	Moderate	Exemption 4
SASI / Select Agent Sensitive Information	HHS* CDC*	2002	Statutory 42 USC 247d	Categories	Designated official	Same	Need-to-know	Moderate	Review / Authorization Exemptions 2, 3
SBU / Sensitive But Unclassified [CDC]	CDC*	7/22/2005	Internal CDC-02 Manual	Categories Examples	Designated official	Same	Need-to-Know	Moderate	Review / Authorization Suggested exs.
SBU / Sensitive But Unclassified [State]	DOS AID DOD*	4/25/2002	Internal 12 FAM 540	Categories FOIA	Supervisory Employees	No policy	Need-to-know Background ck	Moderate	Review
SBU / Sensitive But Unclassified Building Info [GSA]	GSA	3/8/2002	Internal PBS Order 3490.1	Specific categories with examples	Any employee	No policy	Need-to-know	Moderate	Only released with specific authorization
SGI / Safeguards Information	NRC	10/14/1980 Update 11/2/2001	Statutory Atomic Energy Act/10 CFR 73, MD 12.6	Categories Examples	Designated senior officials	Originator	Need-to-know Background ck	High	Review

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
SHSI / Sensitive Homeland Security Information	FAA	2002	Statutory Homeland Sec. Act of 2002	Definition	Designated senior official	Same	Need-to-know State and local officials	Moderate	No release Exemption 3
SHSI / Sensitive Homeland Security Information	NRC	5/28/2002	Internal COMSECY-02-0015	Broad categories, with examples	Designated official	No policy	Need-to-know	Moderate	Review Ashcroft Memo
SSI / Sensitive Security Information [DOT]	DOT/FTA FAA	11/25/2002	Statutory 49 CFR Pt. 15.5	Definition Categories Examples	Senior officials / designated personnel	N/A	Need-to-know	Moderate	No release under Ex. 3 / Administrator's authorization for release
SSI / Sensitive Security Information [USDA]	USDA	1/30/2003	Internal DR 3440-2	Broad definition Categories Restriction	Senior officials	Same / Max 10 yrs	Need-to-know	Moderate	Authorization / suggested exemptions (Ashcroft)
UCNI / Unclassified Controlled Nuclear Information [DOD]	DOD*	10/1990 Updated 9/1998	Statutory 10 USC 128 DoD 5400.7-R	Specific definition/ categories	Senior officials / designees	No policy	Need-to-know US citizen Gov. emp.	Moderate	No release under Exemption 3
UCNI / Unclassified Controlled Nuclear Information [DOE]	DOE	Update 6/30/2000 [internal]	Statutory 42 USC 2168 10 CFR 1017.11 [DOE O471.1A]	Categories, specific	Designated officials	Originator OR FOIA officer	Need-to-know	Moderate	Review
Unclassified Technical Information	DOD*	11/6/1984	Statutory 22 USC 2751 DOD 5230.25	Categories Statutory	Heads of Components	Same	Contractors, need-to-know	N/A	Review Authorization
WMD, other Sensitive Homeland Security Info	TRE DOS	4/4/2002	Internal / Card Memo	Broad definition, categories	N/A	No policy	Need-to-know	Moderate	Ashcroft Memo Exemptions 2, 4

CHART KEY

Policy: Name/acronym for agency's policy regarding unclassified information that is otherwise protected

Agency: Agency or agencies that use the policy listed (where policy features are based on the same documents or authorities, and not merely where the same term is employed to define protected information)

Date: Date of origination date of policy and/or date of update to current policy (where available)

Authority: Statutory/regulatory or internal authority establishing or updating the policy

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

Guidance: Definition and/or other guidance to be followed by individuals in designating information under the policy
Designation: Individual(s) responsible for designating protected information within the agency
Removal: Individual(s) responsible for removing the designation of protected information

- Same: the same individual(s) who are allowed to designate protection are able to remove such protection
- Originator: only the specific individual (and in most cases the individual's supervisor(s) or successor) who made the original designation may remove it

Access: Qualification(s) for individuals who are authorized to access information protected under the policy
Protection: Degree of protection generally applied to documents/electronic media containing information designated under the policy
FOIA: Specific guidelines for treatment of FOIA requests for information protected under the policy

N/A: Not available
No policy: Based on the information collected, the agency's policy includes no specific guidance on this matter

* The information given was not provided by the Agency, but rather is based on our own research or materials submitted by other agencies.

APPENDIX VI
GLOSSARY OF ACRONYMS

ACI–administratively controlled information
AID–Agency for International Development
AIR–Department of the Air Force
ARMY–Department of the Army
ATOMAL–special handling designation for classified information containing atomic materials
CAI–confidential agency information (Environmental Protection Agency)
CBI–confidential business information (Environmental Protection Agency)
CBRN–chemical, radiological, biological, and nuclear (weapons)
CENTCOM–United States Central Command (Army)
CIA–Central Intelligence Agency
CONOPS–U.S. Army Intelligence Command Continental [United States] Operations; continuity of operations
CRS–Congressional Research Service
CUI–controlled unclassified information
DEA–Drug Enforcement Agency
DIA–Defense Intelligence Agency
DOC–Department of Commerce
DOD–Department of Defense
DOE–Department of Energy
DOI–Department of the Interior
DOJ–Department of Justice
DOL–Department of Labor
DOS–Department of State
DOT–Department of Transportation
ECI–enforcement-confidential information (Environmental Protection Agency)
EDU–Department of Education
EO–executive order
EPA–Environmental Protection Agency
EXDIS– Department of State special handling designation, "exclusive distribution to officers with essential need to know"
FAM–Foreign Affairs Manual (Department of State)
FAS–Federation of American Scientists
FBI–Federal Bureau of Investigation
FEMA–Federal Emergency Management Agency
FOIA–Freedom of Information Act
FOUO–for official use only
FRD–formerly restricted data
GAO–Government Accountability Office
GPO–Government Printing Office
GSA–General Services Administration
HHS–Department of Health and Human Services
HIS–homeland security information
HUD–Department of Housing and Urban Development
ISOO–Information Security Oversight Office
LIMDIS–Department of State special handling designation, "Distribution limited to officers, offices, and agencies with the need to know, as determined by the chief of mission or designee"
LOU–limited official use
NARA–National Archives and Record Administration
NASA–National Aeronautics and Space Administration
NATO–North Atlantic Treaty Organization; also special handling designation for NATO classified information
NGA–National Geospatial-Intelligence Agency
NODIS–Department of State special handling designation, "No distribution to other than addressee without approval of addresser or addressee"; used only on messages of the highest sensitivity between the President, the Secretary of State, and Chiefs of Mission.

APPENDIX VI
GLOSSARY OF ACRONYMS

NOFORN–Department of State special handling designation "intelligence which . . . may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nations, or immigrant aliens without originator approval"
NRC–Nuclear Regulatory Commission
NSC–National Security Council
NSF–National Science Foundation
OIP–Office of Information and Privacy, U.S. Department of Justice
OMB–Office of Management and Budget
OPLANS–operation plans
OPM–Office of Personnel Management
OPSEC–operations security
OUO–official use only
PCII–protected critical infrastructure information
PD–Presidential Directive
PROPIN–proprietary information
RD–restricted data
SBA–Small Business Administration
SBU–sensitive but unclassified
SEC–Securities and Exchange Commission
SGI-M–safeguards information-modified handling
SGI–safeguards information
SHSI–sensitive homeland security information
SIOP-ESI–Single Integrated Operations Plan-Extremely Sensitive Information, Department of Defense special handling designation for classified information
SI–sensitive information
SOF–special operations force(s); strategic offensive forces; status of forces
SPECAT–special category designations for classified information, used by Department of Defense
SSA–Social Security Administration
SSI–sensitive security information
SUI–sensitive unclassified information
UCNI–unclassified controlled nuclear information
USDA–U.S. Department of Agriculture
WHS/DFOISR–Department of Defense, Washington Headquarters Services, Directorate of Freedom of Information and Security Review
WMD–weapons of mass destruction