

March 2006

INFORMATION SHARING

The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information





Highlights of [GAO-06-385](#), a report to congressional requesters

Why GAO Did This Study

A number of initiatives to improve information sharing have been called for, including the Homeland Security Act of 2002 and in the Intelligence Reform and Terrorism Prevention Act of 2004. The 2002 act required the development of policies for sharing classified and sensitive but unclassified homeland security information. The 2004 act called for the development of an Information Sharing Environment for terrorism information.

This report examines (1) the status of efforts to establish government-wide information sharing policies and processes and (2) the universe of sensitive but unclassified designations used by the 26 agencies that GAO surveyed and their related policies and procedures.

What GAO Recommends

To provide for information-sharing policies and procedures, GAO recommends that the Director of National Intelligence (DNI) assess progress, address barriers, and propose changes, and that OMB work with agencies on policies, procedures, and controls to help achieve more accountability. OMB said that once ODNI completed its work, OMB would work with ODNI and all agencies on additional steps, if needed. ODNI declined to comment on our report, indicating that the subject matter is outside GAO's purview. We disagree with this assessment because it does not accurately reflect the scope of GAO's statutory authorities.

www.gao.gov/cgi-bin/getrpt?GAO-06-385.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner, 202-512-9286, pownerd@gao.gov or Eileen Larence, 202-512-6510, larencee@gao.gov.

INFORMATION SHARING

The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information

What GAO Found

More than 4 years after September 11, the nation still lacks governmentwide policies and processes to help agencies integrate the myriad of ongoing efforts, including the agency initiatives we identified, to improve the sharing of terrorism-related information that is critical to protecting our homeland. Responsibility for creating these policies and processes shifted initially from the White House to the Office of Management and Budget (OMB), and then to the Department of Homeland Security, but none has yet completed the task. Subsequently, the Intelligence Reform Act called for creation of an Information Sharing Environment, including governing policies and processes for sharing, and a program manager to oversee its development. In December 2005, the President clarified the roles and responsibilities of the program manager, now under the Director of National Intelligence, as well as the new Information Sharing Council and the other agencies in support of creating an Information Sharing Environment by December 2006. At the time of our review, the program manager was in the early stages of addressing this mandate. He issued an interim implementation report with specified tasks and milestones to Congress in January 2006, but soon after announced his resignation. This latest attempt to establish an overall information-sharing road map under the Director of National Intelligence, if it is to succeed once a new manager is appointed, will require the Director's continued vigilance in monitoring progress toward meeting key milestones, identifying any barriers to achieving them, and recommending any necessary changes to the oversight committees.

The agencies that GAO reviewed are using 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect information that they deem critical to their missions—for example, sensitive law or drug enforcement information or controlled nuclear information. For most designations there are no governmentwide policies or procedures that describe the basis on which an agency should assign a given designation and ensure that it will be used consistently from one agency to another. Without such policies, each agency determines what designations and associated policies to apply to the sensitive information it develops or shares. More than half the agencies reported challenges in sharing such information. Finally, most of the agencies GAO reviewed have no policies for determining who and how many employees should have authority to make sensitive but unclassified designations, providing them training on how to make these designations, or performing periodic reviews to determine how well their practices are working. The lack of such recommended internal controls increases the risk that the designations will be misapplied. This could result in either unnecessarily restricting materials that could be shared or inadvertently releasing materials that should be restricted.

Contents

Letter		1
	Results in Brief	4
	Background	7
	The Nation Still Lacks the Governmentwide Policies and Processes Needed to Build an Integrated Terrorism-Related Information-Sharing Road Map, but Smaller-Scale Sharing Initiatives Are Under Way	14
	The Large Number of Sensitive but Unclassified Designations and the Lack of Consistent Policies and Procedures for Their Use Make Sharing Information More Difficult	21
	Conclusions	27
	Recommendations for Executive Action	28
	Agency Comments	29
Appendix I	Objectives, Scope, and Methodology	32
Appendix II	Summary Information on Sensitive But Unclassified Designations by Agency	34
Appendix III	Comments from the Office of the Director of National Intelligence	71
Appendix IV	GAO Contact and Staff Acknowledgments	72
Tables		
	Table 1: Summary of Key Federal Terrorism-Related Information-Sharing Authorities and Initiatives since September 11	9
	Table 2: Sensitive but Unclassified Designations in Use at Selected Federal Agencies	22

Abbreviations

DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
FBI	Federal Bureau of Investigations
FOIA	Freedom of Information Act
FOUO	For Official Use Only
ISE	Information Sharing Environment
IT	information technology
LES	Law Enforcement Sensitive
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PCII	Protected Critical Infrastructure Information
SBU	Sensitive But Unclassified
SSI	Sensitive Security Information

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



United States Government Accountability Office
Washington, DC 20548

March 17, 2006

The Honorable Susan Collins
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Todd Platts
Chairman
Subcommittee on Government Management,
Finance, and Accountability
Committee on Government Reform
House of Representatives

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

House of Representatives

The government's single greatest failure in the lead-up to the September 11, 2001, attacks was the inability of federal agencies to effectively share information about suspected terrorists and their activities, according to the former Vice Chair of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). In addressing this problem, the commission recommended that the sharing and uses of information be guided by a set of practical policy guidelines for sharing that would simultaneously empower and constrain officials, clearly circumscribing what types of information they would be permitted to share as well as the types they would need to protect. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. For these reasons, we recently added information sharing for homeland

security to our list of federal programs and initiatives that pose a relatively high risk to the federal government and that GAO will continue to monitor.¹

Recognizing that information-sharing weaknesses were a major contributing factor to the nation's lack of preparedness for the September 11 attacks, the President has called for a number of information-sharing initiatives driven by two statutory mandates—The Homeland Security Act of 2002² and the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act).³ Section 892 of the Homeland Security Act, enacted in November 2002, requires that the President, among other things, prescribe and implement procedures under which federal agencies can share relevant and appropriate homeland security information with other federal agencies, including the Department of Homeland Security (DHS), and with appropriate state and local personnel, such as law enforcement agencies and first responders. In general, the act defines homeland security information as any information possessed by a federal, state, or local agency that relates to terrorist activities, suspected terrorists, or terrorist organizations, or information that will improve the response to terrorist acts.

In December 2004, Congress mandated a more extensive information-sharing regime through section 1016 of the Intelligence Reform Act, which requires the President to take action to facilitate the sharing of terrorism information by establishing an Information Sharing Environment (ISE) that is to combine policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities and the private sector. The act also requires the President to, among other things, appoint a program manager to oversee development of the ISE and establishes an Information Sharing Council to support the President and the program manager—who is now part of the Office of the Director of National Intelligence (ODNI)—with advice on developing the policies, procedures, guidelines, roles, and standards necessary to implement and maintain the information-sharing environment. In general, the Intelligence Reform Act defines terrorism information as all

¹GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

²Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

³Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

information relating to foreign or international terrorist groups or individuals, or to domestic groups or individuals involved in transnational terrorism, including threats posed by such groups or individuals and communications of or by them, and includes groups or individuals reasonably believed to be associated with such groups or individuals. Subsequent to both of these laws, the President issued a series of executive orders and memorandums that delegated roles and responsibilities for achieving these mandates and set goals and objectives for improving the nation's ability to share homeland security information.

Agencies must often balance the need to share sensitive information, including terrorism-related information, with the need to protect it from widespread access.⁴ Sensitive but unclassified information encompasses a large but unquantifiable amount of information—for example, security plans for federal agency buildings—and other information that does not meet the standards established by executive order for classified national security information but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination. In determining what information to designate as sensitive but unclassified, agencies identify any information they believe must be safeguarded from public release. Such information could include, for example, information in the Department of Justice (DOJ) that is critical to a criminal prosecution. DOJ would protect this information from inappropriate dissemination by designating it Law Enforcement Sensitive and applying prescribed dissemination and handling procedures that correspond with the designation. The Office of Management and Budget (OMB) has primary governmentwide oversight responsibility for such information management and information security policies and programs.

In response to your request to determine the status of information-sharing policy initiatives, we (1) determined the status of efforts to establish governmentwide policies and processes for sharing terrorism-related information between the federal government and its state, local, and private sector partners and (2) identified a universe of different sensitive but unclassified designations that agencies apply to terrorism-related and other sensitive information and determined the extent to which these agencies have policies and procedures in place to ensure their consistent

⁴For purposes of this report, the term “terrorism-related information” encompasses both homeland security information, as defined by the Homeland Security Act, and terrorism information, as defined by the Intelligence Reform Act.

use. To accomplish these objectives, we reviewed relevant laws, directives, and documents and interviewed appropriate officials, including those from ODNI, DHS, and OMB who are involved in federal information-sharing efforts. We also surveyed 26 federal agencies on the types of sensitive but unclassified designations they use and whether they have policies, procedures, and protocols in place for using each designation.⁵ We aggregated the data by agency and sent it back to the agencies for a completeness and accuracy review. Appendix I provides further details on our objectives, scope, and methodology. We performed our work from May 2005 to February 2006 in accordance with generally accepted government auditing standards.

Results in Brief

More than 4 years after September 11, the nation still lacks the governmentwide policies and processes that Congress called for to provide a framework for guiding and integrating the myriad of ongoing efforts to improve the sharing of terrorism-related information critical to protecting our homeland. In part, this is due to the difficulty of the challenge, as well as the fact that responsibility for creating these policies has shifted among various executive agencies. In response to the Homeland Security Act, the White House and OMB were involved in trying to develop guidance on information sharing. Then, in July 2003, the President delegated most of his responsibilities under section 892 of the act to the Secretary of the newly created DHS. Later, DHS decided to reassess its efforts because the more recent Intelligence Reform Act had required creation of an Information Sharing Environment, as part of a more extensive mandate for sharing terrorism information. Most recently, on December 16, 2005, the President issued a new memorandum that, among other things, established guidelines and requirements in support of the Information Sharing Environment. ODNI is in the early stages of addressing its information-sharing mandates and has issued an interim implementation plan to Congress in January 2006 that lays out a number of steps and deadlines for deliverables. According to the interim plan, a large amount of terrorism information is already stored electronically in systems, but there remains an unknown quantity of relevant information not captured and stored electronically. However, many users are not connected to these systems; the information about terrorists, their plans,

⁵We selected major federal agencies defined as those subject to the Chief Financial Officers Act, and also included the Federal Energy Regulatory Commission and the U.S. Postal Service because our previous experience with these agencies indicated that they used sensitive but unclassified designations.

and their activities is fragmentary. The interim plan states that the information-sharing environment will connect the smaller-scale information-sharing initiatives already under way, such as those we identified and discuss later in this report, to take advantage of and build upon what already exists. Accordingly, the President's December 16, 2005, memorandum, after a number of unfulfilled initiatives, establishes an approach and time frames for responding to the mandates to develop governmentwide policies and procedures for information sharing. However, it is unclear what progress will be made because the ODNI program manager announced his resignation on January 26, 2006, and at the time of our review a new program manager had not been named. Once a new program manager is named, ensuring the success of this project will require support and vigilance from ODNI as well as the other agencies mentioned in the memorandum. Consequently, we are recommending that the Director of National Intelligence (DNI) assess progress toward meeting the milestones in the interim plan, identify and address any barriers to progress, and recommend to the congressional oversight committees with jurisdiction any necessary changes so that the goals of the mandates are achieved and the nation has the critical information it needs to protect the homeland.

Federal agencies report using 56 different sensitive but unclassified designations (16 of which belong to one agency) to protect sensitive information—from law or drug enforcement information to controlled nuclear information—and agencies that account for a large percentage of the homeland security budget reported using most of these designations. There are no governmentwide policies or procedures that describe the basis on which agencies should use most of these sensitive but unclassified designations, explain what the different designations mean across agencies, or ensure that they will be used consistently from one agency to another. In this absence, each agency determines what designations to apply to the sensitive but unclassified information it develops or shares. For example, one agency uses the Protected Critical Infrastructure Information designation, which has statutorily prescribed criteria for applying, sharing and protecting the information, whereas 13 agencies designate information For Official Use Only, which does not have similarly prescribed criteria. Sometimes agencies used different labels and handling requirements for similar information and, conversely, similar labels and requirements for very different kinds of information. More than half of the agencies reported encountering challenges in sharing such information. For example, DHS said that sensitive but unclassified information disseminated to its state and local partners had, on occasion,

been posted to public Internet sites or otherwise compromised, potentially revealing possible vulnerabilities to business competitors.

Finally, most agencies do not have limits on who and how many employees have authority to make designations, nor do they have policies for providing training to employees on making designations or performing periodic reviews. Nor are there governmentwide policies that require such internal control practices. Not having these recommended internal controls for effective programs in place increases the probability that the designations could be misapplied, potentially restricting the sharing of material unnecessarily or resulting in dissemination of information that should be restricted. To address this situation, the President in his December 16, 2005, memo gave agencies 90 days to inventory their sensitive but unclassified procedures and report them to the DNI. In carrying out the President's December 16, 2005, mandate, we are recommending that the DNI and the Director of OMB use the results of our work to validate the inventory of designations agencies are required to provide under the memorandum and develop a policy that consolidates designations where possible and addresses the consistent application across agencies. For any designations agencies use, we are also recommending that the Director of OMB, in his oversight role with respect to federal information management, work with other agencies to develop and issue a directive requiring that agencies have internal controls in place that meet GAO's *Standards for Internal Control in the Federal Government*—including implementing guidance, training, and review processes—for effective sensitive but unclassified programs.⁶

We requested comments on a draft of this report from the Director of OMB and the DNI or their designees. OMB neither agreed nor disagreed with our findings and recommendations. OMB commented that once the program manager and others completed their work to establish governmentwide policies, procedures, or protocols to guide the sharing of information as it relates to terrorism and homeland security, they would work with the program manager and all agencies to determine what additional steps are necessary, if any. ODNI, however, declined to comment on our draft report, stating that review of intelligence activities is beyond GAO's purview (see app. III). We do not agree with this assessment. In any event, GAO has broad statutory authority to review

⁶GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

federal programs and activities—including matters related to intelligence activities.

Background

Information sharing is essential to enhance the security of our nation and is a key element in developing comprehensive and practical approaches to defending against potential terrorist attacks. Having information on threats, vulnerabilities, and incidents can help an agency better understand the risks and determine what preventative measures should be implemented. The ability to share such terrorism-related information can also unify the efforts of federal, state, and local government agencies, as well as the private sector in preventing or minimizing terrorist attacks.

The national commission appointed by members of Congress and the President after the September 11 terrorist attacks (the 9/11 Commission) recognized the critical role of information sharing to the reinvigorated mission to protect the homeland from future attacks. In its final report, the commission acknowledged the government has vast amounts of information but a weak system for processing and using it. The commission called on the President to provide incentives for sharing, restore a better balance between security and shared knowledge, and lead a governmentwide effort to address shortcomings in this area.

Since 2001, the President has called for a number of terrorism-related information-sharing initiatives in response to legislative mandates passed by Congress. Relatedly, over the past several years, we have identified potential information-sharing barriers, critical success factors, and other key management issues, including the processes, procedures, and systems to facilitate information sharing between and among government entities and the private sector. Efforts to promote more effective sharing of terrorism-related information must also balance the need to protect and secure it. The executive branch has established requirements for protecting information that is deemed to be critical to our national security.

Laws and Executive Orders Have Established Requirements to Improve Information Sharing since 2001

Since the information-sharing weaknesses of September 11, the President and the Administration have called for a number of terrorism-related information-sharing initiatives driven predominately by two statutory mandates—The Homeland Security Act of 2002⁷ and the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act).⁸ Section 892 of the Homeland Security Act requires that the President, among other things, prescribe and implement procedures under which federal agencies can share relevant homeland security information, as defined in the Homeland Security Act, with other federal agencies, including DHS, and with appropriate state and local personnel, such as law enforcement. Congress subsequently mandated a more extensive information-sharing regimen through section 1016 of the Intelligence Reform Act, requiring that the President take action to facilitate the sharing of terrorism information, as defined in the act, by establishing an Information Sharing Environment (ISE) that will combine policies, procedures, and technologies that link people, systems, and information among all appropriate federal, state, local, and tribal entities, and the private sector. The act also requires the President to, among other things, appoint a program manager to oversee development of the ISE and establishes an Information Sharing Council to support the President and the program manager with advice on developing the policies, procedures, guidelines, roles, and environment. Together, the mandates call for initiatives designed to facilitate the sharing of terrorism-related information—which encompasses both homeland security and terrorism information—within and among all appropriate federal, state, local, and tribal entities, and the private sector. These and other actions are explained in more detail in table 1.

⁷Homeland Security Act of 2002, Pub L. No. 107-296, 116 Stat. 2135.

⁸Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

Table 1: Summary of Key Federal Terrorism-Related Information-Sharing Authorities and Initiatives since September 11

Date	Policy action	Description
Oct. 8, 2001	Executive Order 13228	Established the Office of Homeland Security to, among other things, identify priorities and coordinate efforts for collection and analysis of information, and facilitate the dissemination and exchange of information.
Oct. 26, 2001	USA PATRIOT Act ^a	Mandated broader use of information sharing, access, and dissemination.
July 16, 2002	National Strategy for Homeland Security	Identified information sharing as a foundational element in protecting from, preventing, and responding to potential acts of terrorism.
Nov. 25, 2002	Homeland Security Act of 2002	<p>Created the Department of Homeland Security.</p> <p>Among other things, section 892 defines homeland security information 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 threat. It also requires the President to prescribe and implement procedures under which relevant federal agencies (a) share relevant and appropriate homeland security information with other federal agencies and appropriate state, and local personnel; (b) identify and safeguard homeland security information that is sensitive but unclassified; and (c) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.</p> <p>Section 893 required that the President report, no later than 12 months after enactment, on the implementation of section 892. The report was to include any recommendations for additional measures or appropriation requests to increase the effectiveness of sharing information between and among federal, state, and local entities.</p>
July 29, 2003	Executive Order 13311	Assigned most of the President's information-sharing responsibilities under section 892 of the Homeland Security Act to the Secretary of DHS.
Aug. 27, 2004	Executive Order 13355	Directed the Director of Central Intelligence to establish common security and access standards for managing and handling intelligence systems, information, and products with special emphasis on facilitating the fullest and most prompt sharing of information practicable and the establishment of interface standards for an interoperable information-sharing enterprise.
Aug. 27, 2004	Executive Order 13356 (later revoked by Executive Order 13388)	<p>Required the Director of Central Intelligence, in consultation with the Attorney General and other heads of agencies within the intelligence community, to develop within 90 days common standards for sharing terrorism information, as defined in the order.</p> <p>Established an Information Systems Council, to be chaired by a designee of the OMB Director, to plan for and oversee the establishment of an interoperable terrorism information-sharing environment.</p>
Aug. 27, 2004	Homeland Security Presidential Directive-11	<p>Called for a coordinated and comprehensive approach to terrorist-related screening that supports homeland security.</p> <p>Required that DHS, in coordination with other federal departments and agencies, report within 75 days on plans and progress for enhancing terrorist-related screening, including mechanisms for sharing information among screeners and all relevant government agencies.</p>

Date	Policy action	Description
Dec. 17, 2004	Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act)	<p>Established the Office of the Director of National Intelligence.</p> <p>Section 1016 defines terrorism information as all information—whether collected, produced, or distributed—by intelligence, law enforcement, military, homeland security, or other activities relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or those of other nations; (c) communications of or by such groups or individuals; or (d) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.</p> <p>Section 1016 also requires the President to establish an ISE for terrorism information and to designate a program manager who will, among other things, plan for and oversee implementation of the ISE. It further establishes an Information Sharing Council to assist the President and program manager in their duties under the section.</p>
October 25, 2005	Executive Order 13388	<p>Directs agencies to give the highest priority in their design and use of information systems and in the dissemination of information among agencies to, among other things, facilitate the interchange of terrorism information among agencies and between agencies and appropriate authorities of state, local and tribal governments, and between agencies and appropriate private sector entities.</p> <p>Established an Information Sharing Council, chaired by the program manager, pursuant to section 1016 of the Intelligence Reform Act.</p> <p>Formally revoked Executive Order 13356 but called for the use of standards and plans developed pursuant to that order to facilitate the expeditious and effective implementation of policies set forth in the present order.</p>
December 16, 2005	Memorandum from the President for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment (ISE)	<p>The memorandum directs the DNI to leverage ongoing information-sharing efforts in developing the ISE and provides information-sharing guidelines for: (a) defining common standards for how information is acquired, accessed, shared, and used within the ISE; (b) developing a common framework for sharing information between and among federal agencies; state, local, and tribal governments; law enforcement agencies; and the private sector; (c) standardizing the procedures for sensitive but unclassified information; (d) facilitating the sharing of information between federal agencies and foreign governments; and (e) protecting the information privacy rights and other legal rights of Americans. It also requires that heads of federal agencies actively work to promote a culture of information sharing within their respective agencies.</p> <p>To standardize the procedures for sensitive but unclassified information, the memorandum requires that all agencies inventory their sensitive but unclassified procedures, determine the underlying authority for each procedure, and assess the effectiveness of their existing procedures. Recommendations for standardizing the procedures, based on this information, will subsequently be submitted to the President.</p>

Source: GAO analysis.

^aPublic Law 107-56.

Our Prior Work Identified Challenges in Information Sharing

In January 2005, GAO designated information sharing for homeland security as a governmentwide high-risk area because, although it was receiving increased attention, this area still faced significant challenges. Since 1998, we have recommended the development of a comprehensive plan for information sharing to support critical infrastructure protection efforts.⁹ Key elements of our recommendation can be applied to broader terrorism-related information sharing, including clearly delineating the roles and responsibilities of federal and nonfederal entities, defining interim objectives and milestones, and establishing performance metrics. Over the past several years, we have also issued several reports on challenges related to information sharing.

- In June 2005, we reported that as federal agencies work with state and local public health agencies to improve the public health infrastructure's ability to respond to terrorist threats, including acts of bioterrorism, they faced several challenges.¹⁰ First, the national health information technology (IT) strategy and federal health architecture were still being developed. Second, although federal efforts continue to promote the adoption of data standards, developing such standards and then implementing them were challenges for the health care community. Third, these initiatives involved the need to coordinate among federal, state, and local public health agencies, but establishing effective coordination among the large number of disparate agencies would be a major undertaking.
- In May 2005, we reported that DHS had undertaken numerous initiatives to foster partnerships and enhance information sharing with other federal agencies, state and local governments, and the private sector concerning cyber attacks, threats, and vulnerabilities, but it still needed to address underlying barriers to information sharing.¹¹ At that time, critical infrastructure sector representatives identified as barriers to sharing information with the government fear of release of sensitive information, uncertainty about how the information would be used or protected, lack of trust in DHS, and inconsistency in the usefulness of the information shared by DHS. We made recommendations to the Secretary of Homeland

⁹GAO-05-207.

¹⁰GAO, *Information Technology: Federal Agencies Face Challenges in Implementing Initiatives to Improve Public Health Infrastructure*, GAO-05-308 (Washington, D.C.: June 10, 2005).

¹¹GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

Security to strengthen the department's ability to implement key cybersecurity responsibilities by completing critical activities and resolving underlying challenges.

- In September 2004, we reported that nine federal agencies had identified 34 major networks—32 operational and 2 in development—supporting homeland security functions, including information sharing.¹² The total cost of the networks for which cost estimates were available was approximately \$1 billion per year for fiscal years 2003 and 2004. Among the networks identified, DHS's Homeland Secure Data Network appeared to be a significant initiative for future sharing of classified homeland security information among civilian agencies and DOD.
- In July 2004, we reported on the status of the information sharing and analysis centers that were voluntarily created by the private sector owners of critical infrastructure assets to provide an information-sharing and analysis capability.¹³ The information-sharing center community had identified a number of challenges, including increasing participation, building a trusted relationship, and sharing information between the federal government and the private sector. We recommended that DHS proceed with the development of an information-sharing plan that, among other things, defines the roles and responsibilities of the various stakeholders and establishes criteria for providing the appropriate incentives to address the challenges.
- In October 2001, we identified critical success factors and challenges in building successful information-sharing relationships.¹⁴ In addition, we identified practices that could be applied to other entities trying to develop the means of appropriately sharing information. One of the most difficult challenges to effective information sharing we identified was overcoming new entities' initial reluctance to share. Among the best practices we identified were (1) establishing trusted relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice, (2) developing standards and agreements on how shared information will be used and protected, and

¹²GAO, *Information Technology: Major Federal Networks That Support Homeland Security Functions*, [GAO-04-375](#) (Washington D.C.: Sept. 17, 2004).

¹³GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, [GAO-04-780](#) (Washington, D.C.: July 9, 2004).

¹⁴GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, [GAO-02-24](#) (Washington, D.C.: Oct. 15, 2001).

(3) taking steps to ensure that sensitive information is not inappropriately disseminated.

The Federal Government Has Established Mechanisms to Protect Sensitive Information

The federal government utilizes a variety of policies and procedures, whether prescribed by statute, executive order, or other authority, to limit dissemination and protect against the inadvertent disclosure of sensitive information. For information the government considers critical to our national security, the government may take steps to protect such information by classifying it—for example, Top Secret, Secret, or Confidential—pursuant to criteria established by executive order.¹⁵ The executive order prescribes uniform standards for making all classification decisions across the federal government. Specifically, it prescribes the categories of information that warrant classification, establishes criteria for persons with classification authority, limits the duration of classification decisions, establishes procedures for declassifying or downgrading classified information, prescribes standards for identifying and safeguarding classified materials, requires that agencies prepare classification guides to facilitate proper and uniform classification decisions, and provides for oversight of agency classification decisions.

Information that does not meet the standards established by executive order for classified national security information but that an agency nonetheless considers sufficiently sensitive to warrant restricted dissemination is generally referred to as sensitive but unclassified. In designating information this way, agencies determine that the information they use must therefore be safeguarded from public release. Such information could include, for example, information at DOJ that is critical to a criminal prosecution. DOJ would protect this information from inappropriate dissemination by identifying it with a designation, such as Law Enforcement Sensitive, and prescribing restricted handling procedures for information with this designation. Some specific designations—such as Sensitive Security Information (SSI), used for certain transportation-related information, and Protected Critical Infrastructure Information (PCII), used for information that has been voluntarily submitted to DHS by the private sector and is related to the security of the nation’s critical infrastructure—have a specific basis in statute, but many other designations that agencies use do not. For

¹⁵See Executive Order 13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information* (Mar. 25, 2003).

example, some agencies use the provisions of the Freedom of Information Act (FOIA),¹⁶ which establishes the public's legal right of access to government information but also enables the government to withhold certain information from public release, as their basis for designating information sensitive but unclassified. OMB has primary governmentwide oversight responsibility for information management and information security.¹⁷

The Nation Still Lacks the Governmentwide Policies and Processes Needed to Build an Integrated Terrorism-Related Information-Sharing Road Map, but Smaller-Scale Sharing Initiatives Are Under Way

No governmentwide policies or processes have been established by the executive branch to date to define how to integrate and manage the sharing of terrorism-related information across all levels of government and the private sector despite legislation and executive orders dating back to September 11. This is due, in part, to the difficulty of the challenge, as well as the fact that responsibility for creating these policies has shifted among various executive agencies. Most recently in December 2005, the President once again tried to better clarify the roles and responsibilities of the ODNI program manager, Information Sharing Council, DHS, and other agencies in support of the Information Sharing Environment (ISE). The program manager is in the early stages of addressing the mandate and issued an interim implementation plan to Congress in January 2006 that lays out a number of steps and deadlines for deliverables. However, until governmentwide policies and processes on sharing are in place, the federal government will lack a comprehensive road map to improve the exchange of critical information needed to protect the homeland.

¹⁶5 U.S.C. § 552.

¹⁷OMB is responsible for developing and overseeing federal agency implementation of policies, principles, standards, and guidelines for the management of information resources, including information collection, privacy protection, records management, information security, and information technology. OMB's duties are set forth primarily in the Paperwork Reduction Act (44 U.S.C. § 3504), the Privacy Act (5 U.S.C. § 552a), the Federal Information Security Management Act (44 U.S.C. § 3543), the E-Government Act (44 U.S.C. § 3602), and the Clinger-Cohen Act (40 U.S.C. § 11301). OMB's primary guidance in this area is found in OMB Circular No. A-130, *Management of Federal Information Resources* (November 2000). For this and related OMB guidance, see <http://www.whitehouse.gov/omb/infomag/infopoltech.html>.

Chronology of Efforts to Develop Governmentwide Policies and Processes to Facilitate Terrorism-Related Information Sharing Demonstrates a Series of Unfulfilled Initiatives and the Complexity of the Challenge

Following September 11, the White House and OMB first began to work on information-sharing policies. Following passage of the Homeland Security Act in November 2002, the presidential responsibility for developing policies and processes for information sharing under section 892 of the act was not immediately assigned.

- On July 29, 2003, the President issued Executive Order 13311 delegating to the Secretary of DHS the responsibility to create and implement policies for sharing sensitive homeland security information, and to report to Congress by November 2003 on implementation of section 892 of the Homeland Security Act.
- DHS began its efforts, but did not provide the implementation report to Congress until February 2004. The report primarily discussed several small-scale efforts within DHS associated with sensitive but unclassified information. It did not provide recommendations for additional legislative measures to increase the effectiveness of the sharing of information between and among federal, state, and local entities. The report concluded that to avoid uncertainty and confusion, federal agencies must have a consistent set of policies and procedures for identifying the information to be shared as well as to be safeguarded, but it did not define those policies and procedures or DHS's actions to develop them.
- Subsequently, DHS developed a notice of proposed rule making laying out a proposed policy framework to govern sharing sensitive homeland security information in response to the mandate, but after internal Executive Branch review it was not formally transmitted to OMB and, according to DHS officials, it was never issued.
- When the new Secretary assumed leadership of DHS in February 2005, a reassessment of the proposed rule making was requested in part to assure harmonization with the related requirements of the more recent Intelligence Reform Act, according to DHS's Deputy Director for Information Sharing and Collaboration.

Then, in response to the December 2004 Intelligence Reform Act, the President issued a series of directives to better clarify responsibilities and time frames for achieving a governmentwide road map for information sharing.

- On April 15, 2005, the President designated a program manager responsible for information sharing across the federal government, as required by the Intelligence Reform Act.

-
- On June 2, 2005, the President issued a memorandum directing that during the initial 2-year term of the program manager, the DNI would exercise authority, direction, and control over the program manager. The memorandum also directed the DNI to provide the program manager all personnel, funds, and other resources as assigned. The Intelligence Reform Act had authorized an appropriation of \$20 million for each of fiscal years 2005 and 2006.
 - On October 25, 2005, the President issued Executive Order 13388, which established, among other things, priorities for facilitating the sharing of terrorism information and an Information Sharing Council, chaired by the program manager. The order also revoked the President's earlier direction, Executive Order 13356, which had addressed similar issues and imposed similar requirements with respect to—the Director of Central Intelligence, OMB, and other agencies. The present order, however, calls for the use of standards and plans developed pursuant to the revoked order.
 - In November 2005, the new Information Sharing Council, tasked with planning for and overseeing the establishment of an ISE for sharing terrorism information, had its first meeting and took over for the former Information Systems Council that OMB had chaired.
 - On December 16, 2005, the President issued a memorandum providing guidance and imposing requirements on the heads of all executive departments and agencies in support of the development of the ISE. The memo delineates roles and responsibilities as well as sets deadlines for an effort to leverage ongoing efforts consistent with establishing the ISE as required by the Intelligence Reform Act and in accordance with requirements of the Homeland Security Act and related executive orders. For example, the memorandum requires the program manager, in consultation with the council, to conduct and complete, within 90 days of the memorandum's issuance, a comprehensive evaluation of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies. It also tasked the ODNI with developing the policies, procedures, and architectures needed to create the ISE by December 16, 2006.

The ODNI Is in the Early Stages of Addressing the Intelligence Reform Act Mandate, but Establishing the Required Information-Sharing Requirements Will Be a Challenge

ODNI is in the early stages of addressing the mandate under the Intelligence Reform Act to create an ISE. Soon after the appointment of the program manager in April 2005, he issued a preliminary report on its plans to establish the ISE as required by the act. The program manager later outlined the priorities for his office's work in establishing the ISE:

- clarifying the differing standards among agencies for the designation and dissemination of terrorism information,
- ensuring two-way flow of information from the federal level to the state and local level as well as from state and local agencies to the federal level,
- providing fast-paced, value-added dissemination of information and informational expertise from the intelligence community,
- overcoming the hesitancy of the intelligence community to share information; and
- ensuring the protection of information privacy and other legal rights of Americans, and
- identifying and removing impediments to information sharing.

On January 9, 2006, ODNI issued an *Information Sharing Environment Interim Implementation Plan* to Congress that lays out a number of steps and deadlines for deliverables. ODNI noted in the interim plan the need for more time to develop the final implementation plan because the Intelligence Reform Act requirements call for detailed answers that can be provided only after significant coordination between the program manager and all departments and agencies that are ultimately responsible for implementing the ISE. In the plan, ODNI acknowledged that it recognizes the value and challenge in building ownership for the ISE among all of the federal agencies that have a role in homeland security. The plan also stated that adding to the complexity of the task is the fact that the needs of state, local, and tribal governments and private sector entities must also be taken into account as well. ODNI plans to issue a more comprehensive implementation plan to Congress in July 2006.

The interim plan noted that while a large amount of terrorism information is already stored electronically in systems, many users are not connected to those systems. In addition, there remains an unknown quantity of relevant information not captured and stored electronically. Thus, the information about terrorists, their plans, and their activities is fragmentary. The interim plan states that the ISE will connect disparate

electronic storehouses to take advantage of what already exists. Additionally, it will provide mechanisms for capturing and providing access to terrorism information not currently available electronically. According to the interim plan, ISE implementation will be based on a three-pronged strategy:

- Implementation of the presidential guidelines and requirements.
- Support and augmentation for existing information-sharing environments, such as the National Counterterrorism Center (NCTC). NCTC was selected to serve as one of the initial information-sharing environments because it is the primary organization in the U.S. government for analyzing and integrating all information pertaining to terrorism and counterterrorism.¹⁸ Moreover, DHS and DOJ will identify one or more environments run by states and major urban areas for evaluation of the effectiveness of the flow of terrorism information between federal, state and local governments and the private sector.
- A process for integrating the President's guidelines and requirements with the needs of the broader ISE, which includes addressing the overall ISE's functions, capabilities, resources, conceptual design, architecture, budget, and performance management process.

While recognizing that creating a fully functioning ISE will take time, the interim plan includes a schedule for completing a number of key milestones. For example, by June 14, 2006, the program manager and the Director of NCTC are to have conducted a comprehensive review of all agency missions, roles, and responsibilities related to any aspects of information sharing, especially sharing with state, local, and private entities; developed and disseminated information-sharing standards across the federal, state, local, and private sectors; developed recommendations for sharing with foreign partners and allies; developed privacy guidelines to govern sharing; developed guidelines, training, and incentives to hold personnel accountable for improved information sharing; and developed the ISE investment strategy, among other things.

As part of its efforts to provide end-user input to the technical development of the ISE, ODNI plans to continue to expand the use of information access pilot programs at the state and local levels. Currently,

¹⁸NCTC does not handle intelligence pertaining to domestic terrorism and counterterrorism.

ODNI has two ongoing information-sharing technology pilot programs involving the Federal Bureau of Investigation (FBI) and the Department of Energy (DOE). The FBI's New York Field Office's Special Operations Division is using handheld wireless devices for field operations to facilitate enhanced communications among counterterrorism personnel by providing rapid wireless access to sensitive but unclassified data sources. DOE is sponsoring a pilot project that will apply technical analytic expertise to intelligence pertaining to nuclear terrorism. The project has established a core group of nuclear expert analysts, across five national laboratories, whose focus is on providing both long-term, strategic analysis of potential sources of nuclear terrorism and better short-term tactical intelligence on this issue. Central to the success of this effort is the sharing of all relevant sensitive information with these laboratories.

Despite this progress, when the program manager testified before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, in November 2005, he expressed concern about whether he had enough resources to meet the mandates in the Intelligence Reform Act. For example, he said that for 2006, he did not have a budget line item and was continuing to work with the DNI on his budget. The Intelligence Reform Act authorized \$20 million for fiscal year 2006, but the program manager said he needed \$30 million a year at a minimum. At the time, the program manager also said that although he planned to have a staff of 25, he had only 11 federal employees and 6 contractors on board. On January 26, 2006, the program manager announced his resignation from his position. At the time of our review, a new program manager had not yet been appointed. Once a new program manager is named, it will be important for the DNI to monitor milestones set in the interim implementation plan; identify any barriers to achieving the milestones, such as insufficient resources; and recommend to the oversight committees with jurisdiction any necessary changes to the organizational structure or approach to the ISE.

Many Agencies Are Taking Small-Scale Actions to Improve the Sharing of Terrorism-Related Information

Despite the lack of governmentwide policies and procedures for information sharing, many agencies have their own information-sharing initiatives under way. The following are examples of agency-based terrorism-related information-sharing efforts.

- The FBI leads Joint Terrorism Task Forces, which are one of the means by which the FBI shares information with federal, state, and local law enforcement agencies and officers. At the time of our review, the FBI had 103 Joint Terrorism Task Forces around the country, staffed by bureau

officers as well as state and local law enforcement officers. The mission of the task forces is to respond to terrorism by combining the national and international investigative resources of federal agencies with the street-level expertise of state and local law enforcement agencies.

- The FBI and DHS also collaborate to circulate sensitive intelligence information, through bulletins, to state and local officials. These bulletins are intended to alert state and local governments to information that is being noted at the federal level. As part of this effort, they have provided state and local officials guidance about appropriate control and sharing of this information.

Multiple other mechanisms exist to share terrorism-related information. For example, through our prior work in 2004 we have identified at least 34 major networks that support homeland security functions.¹⁹ Some of the major technology systems we identified in this review and in our other work are described below:

- DHS's Homeland Secure Data Network grew out of a former U.S. Customs Service system that was consolidated with the DHS IT network when the department was created. The system is composed of secure network connections on a data communications framework that connects users to data centers to allow them to share intelligence and other information securely. The network is eventually intended to connect 600 geographically dispersed DHS intelligence-gathering units; operational components; and other federal, state, and local agencies involved in homeland security activities.
- The DOJ Regional Information Sharing System (RISS) links thousands of local, state, and federal law enforcement agencies throughout the nation, providing secure communications, information-sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats. RISS was integrated with the DOJ Law Enforcement Online system in 2002 and with the Automated Trusted Information Exchange in 2003, to provide users with access to homeland security, disaster, and terrorist threat information.

One of the first steps ODNI plans to undertake in developing the ISE is to perform a review of the existing systems such as these so that it can

¹⁹[GAO-04-375](#).

leverage what has already been done and find ways to connect existing systems.

The Large Number of Sensitive but Unclassified Designations and the Lack of Consistent Policies and Procedures for Their Use Make Sharing Information More Difficult

Federal agencies²⁰ report that they are using a total of 56 different designations²¹ for information they determined is sensitive but unclassified, and agencies that account for a large percentage of the homeland security budget reported using most of these designations.²² There are no governmentwide policies or procedures that describe the basis on which agencies should designate, mark, and handle this information. In this absence, the agency determines what designations to apply to its sensitive but unclassified information. Such inconsistency can lead to challenges in information sharing. In fact, more than half of the agencies reported encountering challenges in sharing sensitive but unclassified information. Furthermore, most agencies do not determine who and how many employees can make such designations, provide them training on how to do so, or perform periodic reviews of how well their practices are working, nor are there governmentwide policies that require such internal control practices. By not providing guidance and monitoring, there is a probability that the designation will be misapplied, potentially restricting material unnecessarily or resulting in dissemination of information that should be restricted.

Agencies Report Using 56 Different Designations for Sensitive but Unclassified Information

As table 2 shows, agencies reported using 56 different designations to identify categories of sensitive but unclassified information—including, for example, For Official Use Only (FOUO) and Protected Critical Infrastructure Information (PCII). Most of these designations are in use by agencies that account for a large percentage of the homeland security budget (those shown in bold in the table). However, other agencies in the list, such as the Environmental Protection Agency (EPA) and the U.S. Department of Agriculture (USDA) also have homeland security-related

²⁰We selected major federal agencies—defined as those subject to the Chief Financial Officers Act—and we also included the Federal Energy Regulatory Commission and the U.S. Postal Service because our previous experience with these agencies indicated that they used sensitive but unclassified designations.

²¹This total includes 16 designations used solely by the DOE. DOE also uses four additional designations.

²²The Departments of Defense, Energy, Health and Human Services, Homeland Security, and Justice spent 92 percent of the federal homeland security budget in fiscal year 2005.

sensitive but unclassified information. The numerous designations can be confusing for recipients of this information, such as state and local law enforcement agencies, which must understand and protect the information according to each agency's own rules.

Table 2: Sensitive but Unclassified Designations in Use at Selected Federal Agencies

Designation	Agencies using designation
1 Applied Technology	*Department of Energy (DOE)
2 Attorney-Client Privilege	Department of Commerce (Commerce), * DOE
3 Business Confidential	* DOE
4 Budgetary Information	Environmental Protection Agency (EPA)
5 Census Confidential	Commerce
6 Confidential Information Protection and Statistical Efficiency Act Information (CIPSEA)	Social Security Administration (SSA)
7 Computer Security Act Sensitive Information (CSASI)	Department of Health and Human Services (HHS)
8 Confidential ^a	Department of Labor
9 Confidential Business Information (CBI)	Commerce, EPA
10 Contractor Access Restricted Information (CARI)	HHS
11 Copyrighted Information	* DOE
12 Critical Energy Infrastructure Information (CEII)	Federal Energy Regulatory Commission (FERC)
13 Critical Infrastructure Information	Office of Personnel Management (OPM)
14 DEA Sensitive	Department of Justice (DOJ)
15 DOD Unclassified Controlled Nuclear Information	Department of Defense (DOD)
16 Draft	EPA
17 Export Controlled Information	* DOE
18 For Official Use Only (FOUO)	Commerce, DOD , Department of Education, EPA, General Services Administration, HHS , DHS , Department of Housing and Urban Development (HUD), DOJ , Labor, OPM, SSA, and the Department of Transportation (DOT)
19 For Official Use Only—Law Enforcement Sensitive	DOD
20 Freedom of Information Act (FOIA)	EPA
21 Government Confidential Commercial Information	* DOE
22 High-Temperature Superconductivity Pilot Center Information	* DOE
23 In Confidence	* DOE
24 Intellectual Property	* DOE
25 Law Enforcement Sensitive	Commerce, EPA, DHS , DOJ , HHS , Labor, OPM
26 Law Enforcement Sensitive/Sensitive	DOJ
27 Limited Distribution Information	DOD

Designation	Agencies using designation
28 Limited Official Use (LOU)	DHS, DOJ , Department of Treasury
29 Medical records	EPA
30 Non-Public Information	FERC
31 Not Available National Technical Information Service	Commerce
32 Official Use Only (OUO)	DOE, SSA, Treasury
33 Operations Security Protected Information (OSPI)	HHS
34 Patent Sensitive Information	*DOE
35 Predecisional Draft	*DOE
36 Privacy Act Information	*DOE , EPA
37 Privacy Act Protected Information (PAPI)	HHS
38 Proprietary Information	*DOE, DOJ
39 Protected Battery Information	*DOE
40 Protected Critical Infrastructure Information (PCII)	DHS
41 Safeguards Information	Nuclear Regulatory Commission (NRC)
42 Select Agent Sensitive Information (SASI)	HHS
43 Sensitive But Unclassified (SBU)	Commerce, HHS , NASA, National Science Foundation (NSF), Department of State, U.S. Agency for International Development (USAID)
44 Sensitive Drinking Water Related Information (SDWRI)	EPA
45 Sensitive Information	DOD , U.S. Postal Service (USPS)
46 Sensitive Instruction	SSA
47 Sensitive Internal Use	*DOE
48 Sensitive Unclassified Non-Safeguards Information	NRC
49 Sensitive Nuclear Technology	*DOE
50 Sensitive Security Information (SSI)	DHS, DOT , U.S. Department of Agriculture (USDA)
51 Sensitive Water Vulnerability Assessment Information	EPA
52 Small Business Innovative Research Information	*DOE
53 Technical Information	DOD
54 Trade Sensitive Information	Commerce
55 Unclassified Controlled Nuclear Information (UCNI)	DOE
56 Unclassified National Security-Related [Telecommunications] Information	*DOE

Source: GAO analysis of agency responses.

Note: The designations shown in the table were reported to us by the 26 agencies in our survey as their sensitive but unclassified designations. Three of the agencies reported that they do not have sensitive but unclassified designations. The list may not be all-inclusive because of individual agency interpretations of what constitutes a designation. For example, agencies may use the designation “draft,” but only one reported it as a designation. In addition, DOE has attempted to limit the number of designations it uses, but reported to us that some staff continue to use unofficial designations that they refer to as ad hoc designations. DOE’s ad hoc designations have an asterisk symbol in front of them in the table.

^aThis “confidential” designation does not fall into the classification scheme for national security information established by executive order.

For most of these designations, there are no governmentwide policies or procedures to guide agency decision making on using the designations, explaining what they mean across agencies, and assuring that the information is protected and shared consistently from one agency to another. Different agencies and departments currently define sensitive but unclassified information in many different ways in accordance with their unique missions and authorities.

As a result of the lack of standard criteria for sensitive but unclassified information, multiple agencies often use the same or similar terms to designate information, but they define these terms differently. For example, there are at least 13 agencies that use the designation For Official Use Only, but there are at least five different definitions of FOUO. At least seven agencies or agency components use the term Law Enforcement Sensitive (LES), including the U.S. Marshals Service, the Department of Homeland Security (DHS); the Department of Commerce, and the Office of Personnel Management (OPM). These agencies gave differing definitions for the term. While DHS does not formally define the designation, the Department of Commerce defines it to include information pertaining to the protection of senior government officials, and OPM defines it as unclassified information used by law enforcement personnel that requires protection against unauthorized disclosure to protect the sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

Agencies also use different terminology or restrictive phrases for what is essentially the same type of information. According to a senior official in the Delaware Department of Homeland Security, the multiple designations are a problem. He said that often multiple terms or phrases are used by different agencies for the same material. For example, information about a narcotics-smuggling ring that was financing terrorism might be considered sensitive by the DHS Customs and Border Protection component, which would mark it as FOUO or LES and require it to be kept in a locked file, cabinet, or desk when not in use. The same information might be marked DEA-Sensitive by DOJ's Drug Enforcement Administration (DEA), which under its policy, requires a higher level of protection than normally afforded sensitive but unclassified information. Additionally, the Department of Defense, the Department of State, the Environmental Protection Agency, and the U.S. Agency for International Development all use the categories under FOIA that exempt information from public

disclosure as basic criteria for designating some of its sensitive information. However, for FOIA-exempt material, DOD uses the term For Official Use Only, State uses Sensitive But Unclassified, EPA uses FOIA, and the U.S. Agency for International Development (USAID) uses Sensitive But Unclassified. Use of multiple designations such as this can hamper sharing efforts and confuse end users about the information.

Some Agencies and End Users Reported Challenges in Sharing Sensitive but Unclassified Information

More than half of the agencies reported challenges in sharing sensitive but unclassified information. For example, 11 of the 26 agencies that we surveyed said that they had concerns about the ability of other parties to protect sensitive but unclassified information. These concerns could lead them to share less information than they could. DHS said that sensitive but unclassified information disseminated to its state and local partners had, on occasion, been posted to public Internet sites or otherwise compromised, potentially revealing possible vulnerabilities to business competitors. The Department of Transportation (DOT) said that the time it takes to determine whether other departments' handling and protection requirements meet or exceed DOT's requirements for Sensitive Security Information represents a challenge. Six agencies said that the lack of standardized criteria for defining what constitutes sensitive but unclassified information was a challenge in their efforts to share information, and DOD said that standardizing the designations and definitions used by federal agencies for sensitive but unclassified information might facilitate the handling and safeguarding of the information, thereby strengthening information-sharing efforts. Four agencies reported that they struggle with balancing the trade-off between limited dissemination of sensitive but unclassified information in order to protect it and broader dissemination to more stakeholders, who could use it for their efforts. Finally, 3 agencies reported challenges in using their designations that were not related to identifying, sharing, and safeguarding sensitive information, and 9 agencies reported no challenges.

First responders reported that the multiplicity of designations and definitions not only causes confusion but leads to an alternating feast or famine of information. Lack of clarity on the dissemination rules and lack of common standards for controlling sensitive but unclassified information have led to periods of oversharing of information, often overwhelming end users with the same or similar information from multiple sources, according to an Illinois State Police Officer.

Most of the Agencies We Surveyed Do Not Determine Which Employees Can Make Sensitive but Unclassified Designations, nor Do They Provide These Employees with Training

Of the 20 agencies that reported on who is authorized to make sensitive but unclassified designations at their agency, 13 did not limit which employees could apply at least one of their sensitive but unclassified designations. For example, DHS does not limit which employees may decide whether to designate a document For Official Use Only. At the Department of State, there are no limits on which personnel can designate information as sensitive but unclassified. At the National Aeronautics and Space Administration (NASA), approximately 20,000 civil servants and 80,000 contract employees are authorized to designate information as sensitive but unclassified using the Administratively Controlled Information designation of the agency. In addition, 12 of 23 agencies (or 52 percent) reported that they did not have policies or procedures for specialized training for personnel making sensitive but unclassified designations.

Several agencies, however, have taken steps to limit the number of designators or have provided at least some limited training to their employees. The U.S. Secret Service limits its designation authority solely to those individuals in the organization with the authority to classify information at the Confidential level under the National Security Information program. DOE restricts the application and removal authority for the Unclassified Controlled Nuclear Information (UCNI) designation to specially trained UCNI reviewing officials. Also, the Department of State provides training for its designators, and the Department of the Treasury provides training for designators and users of one of its designations.

Very Few Agencies Perform Periodic Reviews of How Well Their Sensitive but Unclassified Practices Are Working or Set Time Limits on the Designations

Eighteen of the 23 agencies that provided us with information do not have policies or procedures for periodically reviewing how well the agency's designation practices are working and how accurately employees are making these decisions. Without oversight, agencies have no way to know the level of compliance or the effectiveness of the policies and procedures they have set.

In addition, only 2 of the agencies that provided information on the issue of time limits for sensitive but unclassified information set such limits. In contrast, classified national security information is declassified as specified by the governing executive order. The U.S. Postal Service (USPS) set a limit of 5 years, and USDA set a limit of 10 years, after which the designation would no longer be valid, and the information could become publicly available. Two agencies, the General Services Administration and the Department of Commerce, indicated that if it was possible to foresee a specific event that could remove the need for continued protection of the information—for example, a document concerning trade negotiations

would be considered sensitive until the negotiations were ended—the agency marked the document in such a way so that the designation was removed upon the completion of the event. Documents designated sensitive but unclassified at the other agencies that did not set time limits will remain so designated until a review of the document’s status is triggered by an action such as a FOIA request by a private citizen. Continued restriction limits access to this information over the long term.

To address the obstacles to information sharing, the Homeland Security Act required the President to, among other things, develop policies for sharing homeland security information, including sensitive but unclassified information, with appropriate state and local personnel. He delegated this responsibility to the Secretary of the newly created DHS in July 2003. Later, in his December 2005 memo, the President gave agencies 90 days to inventory their sensitive but unclassified procedures and report them to ODNI, which in turn is to provide them to the Secretary of DHS and the Attorney General. Working in coordination with the Secretaries of State, Defense, and Energy and with the DNI, they have 90 days from when they receive the inventories to develop recommended procedures that will provide a more standardized approach for designating homeland security information, law enforcement information, and terrorism information as sensitive but unclassified. The memorandum also requires that ODNI, in coordination and consultation with other agencies, develop recommendations for standardizing sensitive but unclassified procedures for all information not addressed by the first set of recommendations.

Conclusions

In part because of the complexity of the task, shifting responsibilities, and missed deadlines, more than 4 years after September 11 the federal government still lacks comprehensive policies and processes to improve the sharing of information that is critical to protecting our homeland. After the 9/11 Commission’s recommendation that the sharing and uses of information be guided by a set of practical policy guidelines, Congress passed the Intelligence Reform Act and mandated the creation of an Information Sharing Environment (ISE), to be planned for and overseen by a program manager. While recognizing that creating a fully functioning ISE will take time, the program manager’s interim implementation plan includes a schedule for meeting a number of key deadlines. For example, by June 14, 2006, the program manager and the Director of NCTC are to have conducted a comprehensive review of all agency missions, roles, and responsibilities both as producers and users of terrorism information. Given that the program manager resigned and, at the time of our review, a new one had not been appointed, meeting this deadline will be difficult. When a new program manager is appointed, ensuring the success of this

project will require support and vigilance from ODNI as well as the other agencies mentioned in the President's memorandum. It will be essential that the DNI assess progress toward meeting the milestones in the interim plan, identify and address any barriers to progress, and recommend to the congressional oversight committees with jurisdiction any changes necessary to achieve the goals of the mandates.

The President's December 2005 memorandum recognizes the need to standardize procedures for sensitive but unclassified information. Currently, no governmentwide policies or procedures exist for most sensitive but unclassified designations. Our work on the policies and procedures agencies currently use can help validate ODNI's efforts in this area. It will be important that the new policies and procedures provide for consistent application of the designations and consistent handling requirements. Establishing governmentwide policies and procedures is a critical first step, but unless agencies, when implementing designations, ensure employees have the tools they need to use the designations accurately, and establish a monitoring system for their use, designations could be misapplied and information might be unnecessarily restricted or released when it should be protected. In the end, agencies need the flexibility to use designations that meet their mission needs, but where feasible using the same designation and handling procedures across agencies for similar information will provide for more consistent sharing and protection of sensitive information. Without continued vigilance, there is danger that there will be further delays in developing a governmentwide information-sharing policy and in establishing sensitive but unclassified policies that better enable the sharing of the information critical to the protection of the homeland.

Recommendations for Executive Action

To ensure effective implementation of the Intelligence Reform Act, we recommend that the following six actions be taken:

We recommend that the Director of National Intelligence (1) assess progress toward the milestones set in its Interim Implementation Plan; (2) identify any barriers to achieving these milestones, such as insufficient resources and determine ways to resolve them; and (3) recommend to the oversight committees with jurisdiction any necessary changes to the organizational structure or approach to creating the ISE.

In carrying out the President's December 2005 mandates for standardizing sensitive but unclassified information, we recommend that the Director of National Intelligence and the Director of OMB (1) use the results of our

work to validate the inventory of designations that agencies are required to conduct in accordance with the memo and (2) issue a policy that consolidates sensitive but unclassified designations where possible and addresses their consistent application across agencies.

We recommend that the Director of OMB, in his oversight role with respect to federal information management, work with other agencies to develop and issue a directive requiring that agencies have in place internal controls that meet the standards set forth in GAO's Standards for Internal Controls in the Federal Government. This directive should include guidance for employees to use in deciding what information to protect with sensitive but unclassified designations; provisions for training on making designations, controlling, and sharing such information with other entities; and a review process to determine how well the program is working.

Agency Comments

We requested comments on a draft of this report from the Director of OMB and the Director of National Intelligence or their designees. We received comments from OMB that neither agreed nor disagreed with our findings and recommendations. OMB commented that once the program manager and others completed their work to establish governmentwide policies, procedures, or protocols to guide the sharing of information as it relates to terrorism and homeland security, they would work with the program manager and all agencies to determine what additional steps are necessary, if any. ODNI, however, declined to comment on our draft report, stating that the review of intelligence activities is beyond GAO's purview. We are disappointed by the lack of an ODNI response to our report on the critical issue of information-sharing efforts in the federal government. We have placed information sharing for homeland security on GAO's high-risk list, in part because federal agencies have not done an adequate job of sharing critical information in the past and because success in this area will involve the combined efforts of multiple agencies and key stakeholders. The President has tasked ODNI with key coordinating roles in furtherance of this effort.

In declining to comment, ODNI stated that our draft report was "very broad" and that it "addresses a number of intelligence-related issues, including a discussion of the management of [ODNI] and specific recommendations to the Director of National Intelligence (DNI)." ODNI then made a general reference to the DOJ having "previously advised" GAO that "the review of intelligence activities is beyond the GAO's purview." In DOJ's comments on a 2003 GAO report on information

sharing, DOJ similarly said “the review of intelligence activities is an arena beyond GAO’s purview.” However, there was no legal analysis attached to either of these statements.

There is a 1988 DOJ Office of Legal Counsel (OLC) opinion that offers DOJ’s views on our authority to review intelligence activities in the context of foreign policy. In the 1988 opinion, OLC asserted that by enacting the current intelligence oversight framework, codified at 50 U.S.C. § 413, Congress intended the intelligence committees to maintain exclusive oversight with respect to intelligence activities, foreclosing reviews by GAO. Although we recognize that section 413 codified practices to simplify the congressional intelligence oversight process, we do not agree with DOJ’s view that the intelligence oversight framework precludes GAO reviews in the intelligence arena. Neither section 413 nor its legislative history states that the procedures established therein constitute the exclusive mechanism for congressional oversight of intelligence activities, to the exclusion of other relevant committees or GAO. GAO has broad statutory authority to evaluate agency programs and investigate matters related to the receipt, disbursement, and use of public money.²³ GAO also has broad authority to inspect and obtain agency information and records, subject to a few limited exceptions.²⁴

In any event, we do not agree with ODNI’s characterization that our review involved “intelligence activities.” Our review did not involve evaluation of the conduct of actual intelligence activities. Rather, our review addresses the procedures in place to facilitate the sharing of a broad range of information across all levels of government. In our view ODNI’s concept of “intelligence activities” is overly broad and would extend to governmentwide information-sharing efforts clearly outside the traditional intelligence arena—including, for example, procedures for sharing sensitive but unclassified information unrelated to homeland security. The use of such a sweeping definition to limit GAO’s work would seriously impair Congress’s oversight of executive branch information-sharing activities.

²³31 U.S.C. §§ 712, 717.

²⁴These include narrow legal limitations on our access to certain “unvouchered” accounts of the Central Intelligence Agency and on our authority to compel our access to foreign intelligence and counterintelligence information. For more detail, see our testimony, U.S. General Accounting Office, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities*, [GAO-01-975T](#) (Washington, D.C.: July 2001). See also 31 U.S.C. § 716(d).

Given the above, we strongly disagree with ODNI's reasons for declining to comment on our report. ODNI's letter is reprinted in appendix III.

As agreed with your offices, unless you publicly release the contents of this report earlier, we plan no further distribution until 30 days from the report date. We will then send copies of this report to the Director, Office of Management and Budget; the Director of National Intelligence; the Secretaries and heads of the 26 departments and agencies in our review; and interested congressional committees. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact either David Powner at 202-512-9286 or pownerd@gao.gov, or Eileen Larence at 202-512-6510 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



David A. Powner
Director, Information Technology
Management Issues



Eileen Larence
Director, Homeland Security and
Justice

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) determine the status of efforts to establish governmentwide policies and processes for sharing terrorism-related information between the federal government and its state, local, and private sector partners and (2) identify the universe of different sensitive but unclassified designations agencies apply to homeland security and to other sensitive information and determine the extent to which these agencies have policies and procedures in place to ensure their consistent use.

To determine the status of efforts to establish governmentwide policies and processes for sharing terrorism information, we reviewed applicable federal laws, executive orders, presidential directives, memorandums, reports, and testimony. Because they have roles in cross-government information sharing, we also interviewed the Deputy Director and Chief of Staff of the Information Sharing and Collaboration Office at the Department of Homeland Security and the Chief of the Information Policy and Technology Branch, Office of Management and Budget, to determine efforts to date and the current status of required actions. We also interviewed Congressional Research Service staff who work on information-sharing issues and a member of the 9/11 Public Discourse Project, a privately funded continuation of the 9/11 Commission. We gathered publicly available documents on the establishment of the Office of the Director of National Intelligence's (ODNI) on the establishment of the Information Sharing Council and the Information Sharing Environment, met informally with a senior ODNI official who provided us with the interim implementation plan. During the course of our review, we were negotiating protocols for working with ODNI.

We also surveyed 26 major federal agencies, those that are subject to the requirements in the Chief Financial Officers Act as well as the Federal Energy Regulatory Commission and the U.S. Postal Service because our experience with these two agencies indicated that they used sensitive but unclassified designations. We obtained information on their sharing processes for terrorism-related information and for descriptions of any actions they had taken to encourage or improve the sharing of this information. We also asked the agencies about challenges pertaining to identifying, safeguarding, and sharing sensitive but unclassified information. We queried the agencies on the types of sensitive but unclassified designations they use; the policies, procedures, and protocols they have in place for each designation; and the extent to which they provide controls for protecting and policies for sharing these types of information. We aggregated the data by agency and sent them back to the

agencies' responding officials who reviewed the information for completeness and accuracy.

We collected and reviewed applicable federal laws and regulations, policies, procedures, and documents related to the sensitive but unclassified and national security classification processes for federal agencies. We met with officials at the National Archives and Records Administration's Information Security Oversight Office, and discussed policies and processes for handling, overseeing, and sharing national security related information as compared with policies and processes for handling, sharing, and overseeing sensitive but unclassified information. We also contacted the International Association of Police Chiefs, the International Association of Fire Chiefs, and the National Governor's Association to obtain information from end users such as state and local law enforcement, first responders, and state-level homeland security and disaster response agencies, since such organizations are likely to require access to sensitive but unclassified information.

To determine whether appropriate policies and procedures were in place, we relied on GAO's *Standards for Internal Control in the Federal Government* for benchmarks and standards against which to assess each agency's sensitive but unclassified designation policies and procedures.¹ We conducted our work from May 2005 through February 2006 in accordance with generally accepted government auditing standards.

¹[GAO/AIMD-00-21.3.1.](#)

Appendix II: Summary Information on Sensitive But Unclassified Designations by Agency

The following information was provided by the 26 federal agencies that we surveyed. The agencies were queried on the types of sensitive but unclassified designations they use; the basis of the designations; and policies, procedures, and protocols for designating, handling, and sharing these types of information. We provided the agencies with the opportunity to review their summarized information for accuracy and completeness.

Department of Agriculture

Agencywide

Designation: Sensitive Security Information

Basis for designation: Departmental Regulation 3440-2, *Control and Protection of Sensitive Security Information* (January 2003)

Definition: The designation is used for unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity and which describes, discusses, or reflects

- the ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromises, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates federal, state, or local law; harms interstate or international commerce of the United States; or threatens public health or safety;
- any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including—but not limited to—vulnerability assessment, security testing, risk evaluation, risk management planning, or risk audit; or
- any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including—but not limited to—the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element.

Designating authority: Officials from departmental organizations have the authority to determine which information originating under their supervision requires protection against unauthorized disclosure.

Policies or procedures for specialized training for designators: No

Systematic review process: Yes

Department of Commerce

Agencywide

Designation: For Official Use Only

Basis for designation: Freedom of Information Act (FOIA), as amended (5 U.S.C. § 552) Disclosure of Government Information (15 C.F.R. pt. 4), Export Administration Act (EAA) of 1979, as amended (50 U.S.C. app § 2401 et. seq.). (new policy on sensitive but unclassified information in draft Security Manual)

Definition: The designation is used for information that has not been given a security classification, but may be withheld from the public because there is a sound legal basis for withholding the information under specific statutes or regulations.

Designating authority: Secretarial officials, operating unit heads, senior departmental officials, and program managers.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

Designation: Sensitive But Unclassified

Basis for designation: FOIA, as amended; Privacy Act of 1974, as amended (5 U.S.C. § 552a); EAA of 1979, as amended; Tariff Act of 1930, as amended (19 U.S.C. § 1202 et. seq.). (new policy on sensitive but unclassified information in draft Security Manual)

Definition: The designation is used for information the unauthorized disclosure of which could result in harm or unfair treatment to any individual, group or have a negative impact on the department's mission (e.g., personal, medical and financial information, business proprietary information)

Designating authority: Secretarial officials, operating unit heads, senior departmental officials and program managers.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

Designation: Trade Sensitive Information

Basis for designation: Trade Act of 1974, as amended; FOIA, as amended. (new policy on sensitive but unclassified information in draft Security Manual)

Definition: The designation is used for information pertaining to U.S. Trade Policy, strategies and negotiating objectives.

Designating authority: Secretarial officials, operating unit heads, senior departmental officials and program managers.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

Designation: Attorney/Client Privilege

Basis for designation: FOIA, as amended. (new policy on sensitive but unclassified information in draft Security Manual)

Definition: The designation is used for information between an attorney and client; information prepared by an attorney in contemplation of litigation.

Designating authority: Secretarial officials, operating unit heads, senior departmental officials and program managers.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of Commerce (continued)

Designation: Law Enforcement Sensitive

Basis for designation: FOIA, as amended.

(new policy on sensitive but unclassified information in draft Security Manual)

Definition: The designation is used for information pertaining to the protection of senior government officials; investigative data.

Designating authority: Secretarial officials, operating unit heads, senior departmental officials and program managers.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Bureau of Industry and Security

Designation: Confidential Business Information

Basis for designation: FOIA, as amended; Chemical Weapons Convention Implementation Act of 1998 (18 U.S.C. §§ 229-229D; 22 U.S.C. § 6701 et. seq.); Defense Production Act of 1950, as amended (50 U.S.C. app § 2061 et. seq.).

Definition: The designation is used for information designated under the Chemical Weapons Implementation Act of 1998 as a trade secret or commercial financial information, or other information as described in §304(e)(2) of the Act or 5 U.S.C 552 § (b)(4).

Designating authority: Secretarial officials, operating unit heads, senior departmental officials and program managers.

Policies or procedures for specialized training for designators: No

Systematic review process: No

National Technical Information Service

Designation: Not Available National Technical Information Service

Basis for designation: FOIA, as amended

Definition: The designation is used to identify specific technical product information in the NTIS sales collection that has been withdrawn from public disclosure.

Designating authority: Appropriate official of the executive branch agency that authored or funded the report and requests non-disclosure of information to the public.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Bureau of the Census

Designation: Census Confidential

Basis for Designation: Titles 13, 15, and 26, U.S.C.

Definition: The designation is used for information pertaining to statistical collections and survey algorithms used in conduct of mandates of Title 13 U.S.C.

Designating authority: Automatic designation, no designation decision required.

Policies or procedures for specialized training for designators: N/A

Systematic review process: No

Department of Defense

Agencywide

Designation: For Official Use Only Information

Basis for designation: FOIA, as amended; DOD 5200.1-R, *Information Security Program* (January 1997); and Under Secretary of Defense for Intelligence Memorandum, *Interim Information Security Guidance* (April 2004)

Definition: The designation is used as the overall designation for unclassified information that may be withheld from public release under Freedom of Information Act (FOIA) exemptions.

Designating authority: Any DOD employee.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: DOD Unclassified Controlled Nuclear Information

Basis for designation: 10 U.S.C § 128, DOD Directive (DODD) 5210.83, *Department of Defense Unclassified Controlled Nuclear Information*

Definition: The designation is used for unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DOD Special Nuclear Material, equipment, or facilities.

Designating authority: Heads of components and individuals they designate.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Technical Information

Basis for designation: 10 U.S.C. 140c¹, DODD 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure* (November 1984); and DODD 5230.24, *Distribution Statements on Technical Documents* (March 1987)

Definition: DODD 5230.24 requires distribution statements to be placed on technical documents. Distribution statements are used to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations. DODD 5230.24 covers newly created technical documents generated by all DOD-funded research, development, test and evaluation programs and also applies to newly created engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

Designating authority: Managers of technical programs.

Policies and procedures for specialized training for designators: No

Systematic review process: Yes

¹10 U.S.C. § 140c has been renumbered to § 130.

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of Defense (continued)

Designation: Limited Distribution Information

Basis for designation: 10 U.S.C. 455; DODD 5105.60, *National Imagery and Mapping Agency (NIMA)* (October 1996); and DODD 5030.59, *National Imagery and Mapping Agency (NIMA) Limited Distribution Imagery or Geospatial Information and Data* (May 2003) and guidance in DOD 5200.1/R

Definition: Designation used by the National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NGA or information, data, and products derived from such information.

Designating authority: National Geospatial-Intelligence agency personnel.

**Policies or procedures for specialized training for
designators:** Yes

Systematic review process: Yes

Designation: For Official Use Only—Law Enforcement Sensitive

Basis for designation: DOD 5200.1-R, *Information Security Program* (January 1997), and Under Secretary of Defense for Intelligence Memorandum, *Interim Information Security Guidance* (April 2004)

Definition: The designation is used for certain information compiled for law enforcement purposes that should be afforded appropriate security in order to protect certain legitimate government interests.

Designating authority: Personnel engaged in law enforcement activities.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of Defense (continued)

Designation: Sensitive Information

Basis for designation: Computer Security Act of 1987, Pub. L. No. 100-235, (as enacted at 15 U.S.C. § 271 et. seq.);² DOD 5200.1-R, *Information Security Program* (January 1997), and Under Secretary of Defense for Intelligence Memorandum, *Interim Information Security Guidance* (April 2004)

Definition: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.

Designating authority: Personnel involved with information systems.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

²Section 303 of the Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2957-59, in effect repealed portions of the Computer Security Act relevant to this discussion by amending the language 15 U.S.C. § 278g-3 in its entirety, to the exclusion of the “sensitive information” definition.

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

Department of Education

Agencywide

Designation: For Official Use Only

Basis for designation: FOIA, as amended; Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501, note); Handbook for Information Technology Security Risk Assessment Procedures OCIO-07 (January 2004); and Handbook for Information Assurance Security OCIO-01 (December 2005)

Definition: The designation is used for information that (1) falls within one or more of the nine exemptions or three exclusions of the Freedom of Information Act (FOIA), (2) is protected by the Privacy Act of 1974, or (3) is marked by the Office of the Inspector General to prohibit distribution to unauthorized persons.

Designating authority: The owner of the information.

Policies and procedures for specialized training for designators: No

Systematic review process: No

Department of Energy³

Agencywide

Designation: Official Use Only

Basis for designation: DOE Order 471.3 (April 2003)

Definition: Certain unclassified information that may be exempt from public release under the Freedom of Information Act and has the potential to do damage to governmental, commercial or private interests if disseminated to people who do not need the information to perform their jobs or other DOE authorized functions.

Designating authority: Any DOE or DOE contractor employee.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Unclassified Controlled Nuclear Information

Basis for designation: Section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2168), 10 C.F.R. pt.1017, DOE Order 471.1A (June 2000)

Definition: The designation is used for certain unclassified government information prohibited from unauthorized dissemination under section 148 of the Atomic Energy Act

- which concerns atomic energy defense programs
- which pertains to (i) the design of production or utilization facilities (ii) security measures for the physical protection of production or utilization facilities or nuclear material contained in these facilities or in transit (iii) the design, manufacture or utilization of nuclear weapons or components that were once classified as Restricted Data
- whose unauthorized dissemination could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of (i) illegal production of nuclear weapons or (ii) theft, diversion, or sabotage of nuclear materials, equipment or facilities.

Designating authority: UCNI reviewing officials (training and designated individuals in DOE and DOE contractor organizations) only.

Policies or Procedures for Specialized Training for Designators: Yes

Systematic review process: No

³The Department of Energy reported that, although it has attempted to limit the number of designations it uses, some staff continue to use some informal designations that they refer to as ad hoc designations. They are as follows: Applied Technology, Attorney/Client Privileged Information, Business Confidential, Copyrighted Information, Export Controlled Information, Government Confidential Commercial Information, High-Temperature Superconductivity Pilot Center Information, In Confidence, Intellectual Property, Patent Sensitive Information, Predecisional Draft, Privacy Act Information, Proprietary Information, Protected Battery Information, Sensitive Internal Use, Sensitive Nuclear Technology, Small Business Innovative Research Information, and Unclassified National Security-Related [Telecommunications] Information.

Department of Health and Human Services

Agencywide

Designation: Sensitive But Unclassified

Basis for designation: FOIA, as amended; Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Titles 7, 21, 29, and 42, U.S.C.; see 21 U.S.C. § 350c)
(Draft HHS Information Security Policy and Procedures for Sensitive But Unclassified Information)

Definition: The Sensitive But Unclassified designation is used for information that does not meet the standards for classification under national security information but it is protected from public disclosure under exemptions 2-8 of FOIA.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Centers for Disease Control and Prevention

Designation: Sensitive But Unclassified

Basis for designation: Section 201(a) of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, (42 U.S.C. § 262a (h)), and 42 C.F.R. pt. 73 (Select Agents and Toxins)
(new policy in draft)

Definition: The designation is used for information which identifies possession, use, or transfer of a select agent or toxin; or information derived therefrom to the extent that it identifies the listed agent or toxin possessed, used, or transferred by a specified registered person or discloses the identity or location of a specific registered person.

Designating authority: Not specified

Policies or procedures for specialized training for designators: N/A

Systematic review process: N/A

Designation: Computer Security Act Sensitive Information

Basis for designation: Computer Security Act of 1987
(new policy in draft)

Definition: The designation is used for any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, U.S.C. (the Privacy Act).

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Centers for Disease Control and Prevention (continued)

Designation: Contractor Access Restricted Information

Basis for designation: 41 U.S.C. § 401⁴; Federal Acquisition Regulations 1.102; Executive Order 11222 (May 8, 1965)
(new policy in draft)

Definition: Unclassified information that involves functions reserved to the federal government as vested by the Constitution as inherent power or as implied power as necessary for the proper performance of its duties.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: For Official Use Only

Basis for designation: FOIA, as amended
(new policy in draft)

Definition: This designation is applied to unclassified information that is exempt from mandatory release to the public under FOIA.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Law Enforcement Sensitive

Basis for designation: Not specified
(new policy in draft)

Definition: The designation is used for law enforcement purposes. Information that could reasonably be expected to interfere with law enforcement proceedings, would deprive a person of a right to a fair trial or impartial adjudication, could reasonably be expected to constitute an unwarranted invasion of personal privacy of others, disclose the identity of a confidential source, disclose investigative techniques and procedures or could reasonably be expected to endanger the life or physical safety of any individual is to be marked law enforcement sensitive.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Operations Security Protected Information

Basis for designation: National Security Decision Directive 298, (January 1988).
(new policy in draft)

Definition: The designation is applied to unclassified information concerning CDC mission, functions, operations, or programs that require protection in the national interest, or security of homeland defense.

⁴See Federal Acquisition Reform Act of 1996, Pub. L. No. 104-106, § 4305(a)(2), 110 Stat. 186, 665 (repealing 41 U.S.C. § 401).

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Centers for Disease Control and Prevention (continued)

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Privacy Act Protected Information

Basis for designation: Privacy Act of 1974, as amended: 45 C.F.R. pt. 5b
(new policy in draft)

Definition: The designation covers information that, if released, could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Select Agent Sensitive Information

Basis for designation: Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
(new policy in draft)

Definition: The designation is used on any document that has been prepared using information from the Select Agent Program database and identifies more than one entity as having an unspecified select agent or agents. A portion of the Select Agent Program data base, or any document that has been prepared using information from the Select Agent Program database and is limited to information received from one entity will be unclassified but will be protected to safeguard the public interest and marked as For Official Use Only.

Designating authority: Not specified

Policies or procedures for specialized training for designators: No

Systematic review process: No

Department of Homeland Security

Agencywide

Designation: For Official Use Only

Basis For designation: Management Directive 11042.1 (January 2005)

Definition: The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely affect a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest.

Designating authority: Any DHS employee, detailee, or contractor.

Policies or procedures for specialized training for designators: Yes

Systematic review process: No

Designation: Law Enforcement Sensitive

Basis for designation: Not specified.

Definition: The designation is not formally defined by a DHS policy, directive, or regulation. In practice, according to DHS, its law enforcement components apply the designation to information that may be exempt from disclosure under exemptions 2 or 7 of the Freedom of Information Act.

Designating authority: Any DHS employee, detailee, or contractor attached to a component with a law enforcement mission.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Directorate for Preparedness

Designation: Protected Critical Infrastructure Information

Basis for designation: 6 C.F.R § 29.2 (February 2004)

Definition: The designation is defined as information (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in 6 C.F.R § 29.5.

Designating authority: PClI Program Manager or authorized designees.

Policies or procedures specialized training for designators: N/A

Systematic review process: No

Transportation Security Administration & U.S. Coast Guard

Designation: Sensitive Security Information

Basis for designation: Homeland Security Act of 2002 (Pub. L. No.107-296); Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295), 49 U.S.C. § 114(s); 49 C.F.R. pt.1520 (May 2004); Management Directive (MD) 11056 (December 2005).

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of Homeland Security (continued)

Definition: In accordance with 49 U.S.C. § 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Transportation Security Administration has determined would 1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

Designating authority: All TSA personnel and contractors are obligated to mark information SSI if it fits within the rules established by 49 C.F.R. § 1520.5. The TSA Administrator and four other TSA personnel have the discretion to designate information outside the rules. See § 1520.5(b)(16).

Policies or procedures for specialized training for designators: Yes	Systematic review process: No
---	--------------------------------------

US Secret Service

Designation: Limited Official Use

Basis For designation: USSS Recruitment and Personnel Security Manual

Definition: The designation, Limited Official Use, administratively controls officially limited information within the agency as it relates to internal investigations, and the development of Secret Service or DHS policy. This includes information pertaining to (1) the enforcement of criminal/civil law relating to departmental or bureau matters, (2) departmental or bureau personnel rules and regulations, and (3) sensitive or proprietary information relative to departmental or bureau policy.

Designating authority: Only persons authorized to classify documents as Confidential are authorized to designate documents as LOU.

Policies or procedures for specialized training for designators: Yes	Systematic review process: No
---	--------------------------------------

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

Department of Housing and Urban Development

Agencywide

Designation: For Official Use Only

Basis for designation: None (new policy in draft)

Definition: None at present.

Designating authority: Not specified.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of the Interior

Agencywide

Designation: None

Basis for designation: N/A (new policy in draft)

Definition: N/A

Designating authority: N/A

**Policies or procedures for specialized training for
designators:** N/A

Systematic review process: N/A

Department of Justice

Agencywide (Justice Management Division)

Designation: Limited Official Use

Basis for designation: DOJ Order 2620.7 (September 1982)

Definition: Unclassified information of a sensitive, proprietary, or personally private nature which must be protected against release to unauthorized individuals.

Designating authority: Heads of Departmental organizations or their designees.

Policies or procedures for specialized training for designators: No

Systematic review process: No

US Marshals Service

Designation: Law Enforcement Sensitive

Basis for designation: USMS Policy Directive 2.34 (November 2005)

Definition: The law enforcement sensitive designation is used for unclassified information of a sensitive and proprietary nature that if disclosed could cause harm to law enforcement activities by jeopardizing investigations, compromising operations, or causing life-threatening situations for confidential informants, witnesses, or law enforcement personnel. The Agencywide Limited Official Use designation is used for other sensitive, but unclassified, official information.

Designating authority: Supervisors and management only.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Bureau of Alcohol, Tobacco, Firearms and Explosives

Designation: Law Enforcement Sensitive/ Sensitive

Basis for designation: DOJ Order 2620.7 (September 1982); ATF Order 3700.2A; and ATF Order 7500.2

Definition: The designation is used for information that, if disclosed, could adversely affect the ability of ATF/NDIC to accomplish its mission.

Designating authority: Not specified in response.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Drug Enforcement Administration

Designation: DEA Sensitive

Basis for designation: Control and Decontrol of DEA Sensitive Information (June 1999)

Definition: The designation is used for information that, if disclosed, could adversely affect the ability of DEA to accomplish its mission and when disseminated outside the agency, must be afforded a higher level of protection than Sensitive But Unclassified information.

Designating authority: Special Agents in Charge, Assistant Special Agents in Charge, Resident Agents in Charge, Group Supervisors, Laboratory Chiefs, Section Chiefs and higher, DEA Inspectors, and DEA Strike Force Representatives occupying supervisory and liaison positions.

Policies or procedures for specialized training for designators: Yes

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

**Department of Justice (continued)
Federal Bureau of Prisons**

Designation: For Official Use Only

Basis for designation: BOP Policy 1237.11 (October 1997)

Definition: The BOP would designate the following information as FOUO:

- internal personnel rules and practices,
- information exempt from disclosure (i.e. inmate medical data),
- privileged interagency correspondence,
- medical and personnel files,
- LES information,
- certain financial data.

Designating authority: BOP agency head and facility heads or equivalent.

**Policies or procedures for specialized training for
designators:** Yes

Systematic review process: No

Federal Bureau of Investigation

Designation: For Official Use Only

Basis for designation: Intelligence Policy Manual (August 2005)

Definition: The designation is used for information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C. 552.

Designating authority: Any FBI employee or contractor in the course of performing assigned duties may designate information as FOUO.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

Designation: Law Enforcement Sensitive

Basis for designation: Intelligence Policy Manual (August 2005)

Definition: The designation is used to protect information compiled for law enforcement purposes. LES is a subset of FOUO.

Designating authority: Any FBI employee or contractor in the course of performing assigned duties may designate information as LES.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

Designation: Limited Official Use

Basis for designation: DOJ Order 2620.7, Control and Protection of Limited Official Use Information (September 1982)

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Federal Bureau of Investigation (continued)

Definition: The designation is used for unclassified information of a sensitive, proprietary, or personally private nature which must be protected against release to unauthorized individuals.

Designating authority: Any FBI employee or contractor in the course of performing assigned duties may designate information as LOU under guidelines of DOJ Order.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

Designation: Proprietary Information

Basis for designation: Director of Central Intelligence Directive (DCID) 6/6, Security Controls on the Dissemination of Intelligence Information (July 2001)

Definition: The designation is used for information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This marking may be used on government proprietary information only when the government proprietary information can provide a contractor(s) an unfair advantage, such as US Government budget or financial information.

Designating authority: Any FBI employee or contractor in the course of performing assigned duties may designate information meeting the DCID criteria as PROPIN.

Policies or procedures for specialized training for designators: No	Systematic review process: No
--	--------------------------------------

Department of Labor
Bureau of Labor Statistics

Designation: Confidential

Basis for designation: Confidential Information Protection and Statistical Efficiency Act (Title V of Pub. L. No.107-347, see 44 U.S.C. § 3501, note; Trade Secrets Act (see 18 U.S.C. § 1905); Privacy Act, as amended; OMB Statistical Confidentiality Order (62 FR 35043, June 27, 1997), OMB Statistical Directive No. 3, Secretary's Order 39-72, Commissioner's Order No. 3-04, Commissioner's Order 4-00, Commissioner's Order 1-05 and Administrative Procedures 2-05

Definition: The designation is used for information acquired from respondents to BLS statistical surveys under a pledge of confidentiality for exclusively statistical purposes. It is also used for pre-release economic series data, which are statistics and analyses that have not yet officially been released to the public. This includes, in particular, pre-release economic data for the Principal Federal Economic Indicators produced by the Bureau.

Designating authority: Commissioner of Labor Statistics

Policies and procedures for specialized training for designators: N/A

Systematic review process: N/A

Office of Inspector General

Designation: Law Enforcement Sensitive

Basis for designation: The Inspector General's Act of 1978, as amended (5 U.S.C. app. 3)

Definition: Investigative information involving the progression of a case from intelligence gathering through the referral for prosecution.

Designating authority: Automatic designation under the Inspector General Act of 1978

Policies and procedures for specialized training for designators: No

Systematic review process: No

Designation: For Official Use Only

Basis for designation: The Inspector General's Act of 1978

Definition: Also used for Law Enforcement Sensitive information when memorandums/letters are provided to Federal entities and for when an investigative memorandum is forwarded to a Department of Labor agency for their review and decision on the outcome of an investigation.

Designating authority: Not specified

Policies and procedures for specialized training for designators: No

Systematic review process: No

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

Department of State
Agencywide

Designation: Sensitive But Unclassified

Basis for designation: FOIA, as amended; Privacy Act, as amended; 12 FAM 540 (November 2005)

Definition: Information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons. Sensitive But Unclassified information should meet one or more of the criteria for exemption from public disclosure under the Freedom of Information Act (FOIA) (which also exempts information protected under other statutes), 5 U.S.C. § 552 or should be protected by the Privacy Act, 5 U.S.C. § 552a.

Designating authority: All Department of State personnel.

**Policies or procedures for specialized training for
designators:** Yes

Systematic review process: No

Department of the Treasury

Agencywide

Designation: Limited Official Use

Basis for designation: Treasury Security Manual (June 1998)

Definition: Information that an authorized official within the Department determines needs to be protected from unauthorized disclosure because such disclosure would injure the Department's mission or responsibilities, or cause harm to other persons or parties. LOU includes—but is not necessarily limited to—important, delicate, sensitive, or proprietary information used in development of Treasury policy, such as the enforcement of criminal and civil laws relating to Treasury operations and the consideration of financial information provided in confidence.

Designating authority: Any Treasury employee may designate information Limited Official Use.

Policies and procedures for specialized training for designators: Yes

Systematic review process: No

Internal Revenue Service

Designation: Limited Official Use

Basis for designation: Internal Revenue Manual 11.3.12 (July 2005)

Definition: The designation is used only on materials intended for use by the highest officials within the Internal Revenue Service or addressed to officials of the Department of the Treasury.

Designating authority: Documents may be classified LOU only by the Commissioner.

Policies and procedures for specialized training for designators: No

Systematic review process: No

Designation: Official Use Only

Basis for designation: Internal Revenue Manual 11.3.12 (July 2005)

Definition: The designation is used for certain types of documents that should not be subject to public distribution such as printed materials intended for internal use and the law enforcement manual.

Designating authority: Not specified.

Policies and procedures for specialized training for designators: No

Systematic review process: No

Department of Transportation

Agencywide

Designation: For Official Use Only (FOUO)

Basis for designation: 5 U.S.C. § 301; 49 U.S.C. § 322; DOT M 1640-4D (December 1997)

Definition: DOT uses the general description and terms contained in the Freedom of Information Act, including the first seven exemptions from public disclosure of information, as its basis for designating information as FOUO.

Designating authority: Any DOT employee

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

Designation: Sensitive Security Information

Basis for designation: 49 U.S.C. § 40119(b), 49 C.F.R. pt.15

Definition: SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which [the Transportation Security Administration] has determined would (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to transportation safety.

Designating authority: All modal administrators and their designees (designation must be done in writing).

**Policies or procedures for specialized training for
designators:** Yes

Systematic review process: Yes

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Department of Veterans Affairs

Agencywide

Designation: None

Basis of designation: N/A

Definition: N/A

Designating authority: N/A

**Policies or procedures for specialized training for
designators:** N/A

Systematic review process: N/A

Environmental Protection Agency

Agencywide

Designation: Law Enforcement Sensitive	
Basis for designation: FOIA, as amended	
Definition: The designation is used for records or information compiled for law enforcement purposes, including information that relates to investigative procedures and grand jury information. It aligns with the definition of Freedom of Information Act exemption 7 (records or information compiled for law enforcement purposes).	
Designating authority: Not specified.	
Policies or procedures for specialized training for designators: No	Systematic review process: No
Designation: Freedom of Information Act	
Basis for designation: FOIA, as amended; Freedom of Information Act Manual (EPA Directive 1550) (1992)	
Definition: The designation is used for information defined exempt pursuant to FOIA and related case law.	
Designating authority: Not specified.	
Policies or procedures for specialized training for designators: No	Systematic review process: No
Designation: Privacy Act	
Basis for designation: Privacy Act, as amended; Privacy Act Manual (EPA Directive 2190) (1986).	
Definition: The designation is used for information defined pursuant to the Privacy Act and implementing regulations.	
Designating authority: Not specified.	
Policies or procedures for specialized training for designators: No	Systematic review process: No
Designation: Medical Records	
Basis for designation: Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191)	
Definition: The designation is used for information defined pursuant to the Health Insurance Portability and Accountability Act (HIPPA) of 1996.	
Designating authority: Not specified.	
Policies or procedures for specialized training for designators: No	Systematic review process: No
Designation: Budgetary Information	
Basis for designation: Information Sensitivity Compendium (Guidance Document)	
Definition: The designation is used for information defined pursuant to OMB Circular A-11, prohibition of release of agency budget information before public release of the President's budget.	
Designating authority: Not specified	
Policies or procedures for specialized training for designators: No	Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Environmental Protection Agency (continued)

Designation: Confidential Business Information

Basis for designation: Resource Conservation and Recovery Act, as amended (42 U.S.C. § 6901 et. seq.); CBI Manual/Security Plan; Toxic Substances Control Act, as amended (see 15 U.S.C. § 2601 et. seq.)

Definition: The designation is used for information defined by the Agency under various statutes and covered under FOIA exemption 4.

Designating authority: EPA's contracting officers may designate information as CBI, as well as the owner of the information.

Policies or procedures for specialized training for designators: Yes

Systematic review process: No

Designation: Sensitive Water Vulnerability Assessment Information

Basis for designation: Information Protection Protocol (November 2002)

Definition: The designation is used to control access to vulnerability assessments and information derived from the vulnerability assessments provided to EPA in accordance with the Public Health Safety and Bioterrorism Preparedness and Response Act of 2002.

Designating authority: The EPA Administrator designates those who will have access and control.

Policies or procedures for specialized training for designators: Yes

Systematic review process: No

Designation: Sensitive Drinking Water-Related Information

Basis for designation: FOIA, as amended; Policy to Manage SDWRI (April 2005)

Definition: The designation is used for information pertaining to drinking water well and intake location data and the source water area GIS polygon coverages as sensitive related to homeland security.

Designating authority: Not specified.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Draft

Basis for designation: No specific authority

Definition: The designation is used for general information that should be handled with care.

Designating authority: Not specified.

Policies or procedures for specialized training for designators: No

Systematic review process: No

National Homeland Security Research Center

Designation: For Official Use Only

Basis For designation: NHSRC-70-01, Rev.0 (November 2004)

Definition: For Official Use Only (FOUO) is applied by the NHSRC as the sole designator for sensitive but unclassified (SBU) information. The NHRSC uses the following definition of sensitive but unclassified, taken from the Computer Security Act of 1987, Public Law 100-235, which defines "sensitive information" as "any information, the

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5 [U.S.C.] (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”.

Designating authority: Any National Homeland Security Research Center employee, contractor, subcontractor, or grantee may designate information FOUO. However, such designations must be certified by a NHSRC Review Authority (DRA).

Policies or procedures for specialized training for designators: Yes

Systematic review process: Yes

Federal Energy Regulation Commission

Agencywide

Designation: Critical Energy Infrastructure Information

Basis for designation: FOIA, as amended; 18 C.F.R. §§ 388.112-.113; and Commissioner Order Nos. 630, 630-A, 649, and 662.

Definition: Information about proposed or existing critical infrastructure that

- relates to the production, generation, transportation, transmission, or distribution of energy;
- could be useful to a person in planning an attack on critical infrastructure;
- is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. § 552; and
- does not simply give the location of the critical infrastructure.

Designating authority: Both filers and staff can mark information CEII.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Non-Public Information

Basis for designation: FOIA, as amended; 18 C.F.R. §§ 1b.9, 1b.20-.21(c), 385.410, 606, 388.112; 15 U.S.C. § 717g(b), 16 U.S.C. 825(b)

Definition: Any information that is not routinely provided to the public absent a Freedom of Information Act (FOIA) request, including information that would not be released under the FOIA. Non-Public Information includes, for example,

- information that is submitted to the Commission with a request for non-public treatment under 18 C.F.R. § 388.112(a), which applies to information the submitter claims is exempt from mandatory disclosure under the FOIA.
- information concerning dispute resolution communications. See 18 C.F.R. § 385.606.
- information covered by a protective order. See 18 C.F.R. § 385.410.
- information obtained during the course of an investigation. See 18 C.F.R. §§ 1b.9, 1b.20.
- Information and documents obtained through the Hotline Staff. See 18 C.F.R. § 1b.21(c).
- information obtained during the course of examination of books or other accounts. See 15 U.S.C. § 717g(b); 16 U.S.C. § 825(b).
- information exempt from disclosure under the FOIA, such as drafts; staff deliberative documents; attorney work product and attorney-client communications exempt from disclosure under 5 U.S.C. § 552(b)(5).

Designating authority: All filers and staff

Policies or procedures for specialized training for designators: No

Systematic review process: No

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

General Services Administration

Agencywide

Designation: For Official Use Only

Basis For designation: GSA Order, PBS 3490.1—applicable only to building information (March 2002—new overall policy in draft)

Definition: This designation is used for building information deemed sensitive and includes but is not limited to paper or electronic documentation of physical facility information.

Designating authority: Assistant Regional Administrators and the Chief Architect.

Policies or procedures for specialized training for designators: Yes	Systematic review process: No
---	--------------------------------------

National Aeronautics and Space Administration

Agencywide

Designation: Sensitive But Unclassified

Basis for designation: Computer Security Act of 1987; Privacy Act, as amended; and NPR 1600.1 (November 2005)

Definition: Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects, or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations:

- ITAR—International Traffic in Arms Regulations
- EAR—Export Administration Regulations
- MCTL—Militarily Critical Technologies List
- FAR—Federal Acquisition regulations
- Privacy Act
- Proprietary
- FOIA—Freedom of Information Act
- UCNI—Unclassified Controlled Nuclear Information
- NASA Developed Software
- Scientific and Technical Information (STI)
- Source Selection and Bid and Proposal Information
- Inventions

Designating authority: All NASA employees and contractors.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

National Science Foundation

Agencywide

Designation: Sensitive But Unclassified

Basis for designation: NSF Privacy Regulations (45 C.F.R. § 613), NSF Freedom of Information Act Regulations (45 C.F.R. § 612), NSF Bulletin 05-14 (September 2005)

Definition: The designation is given to information that is defined as sensitive under the Privacy Act.

Designating authority: Not specified in response.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

Nuclear Regulatory Commission

Agencywide

Designation: Safeguards Information

Basis for designation: Section 147 of Atomic Energy Act of 1954, as amended (42 U.S.C. § 2167); 10 C.F.R. § 73-21; Directive 12.6 (December 1999)
(policy revision in draft)

Definition: Safeguards Information means information, not otherwise classified as National Security Information or Restricted Data that specifically identifies a licensee's or applicant's detailed

- control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security;
- security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or
- security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility.

Designating authority: Employees at the section chief and above levels.

Policies or procedures for specialized training for designators: Yes

Systematic review process: No

Designation: Sensitive Unclassified Non-Safeguards Information

Basis for designation: NRC Policy for Handling, Marking and Protecting SUNSI (October 2005)

Definition: Sensitive but unclassified information that does not pertain to nuclear Safeguards Information, including any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and federal programs, or the personal privacy of individuals.

Designating authority: Variable.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Office of Personnel Management

Agencywide

Designation: For Official Use Only

Basis for designation: Not specified
(policy is in draft)

Definition: The term used within OPM to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely affect a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest.

Designating authority: Deputy Associate Director of the Center for Security and Emergency Actions (CSEA).

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Law Enforcement Sensitive

Basis for designation: Not specified

Definition: Law Enforcement Sensitive Information is unclassified information used by law enforcement personnel and requires protection against unauthorized disclosure to protect the sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. Law Enforcement Sensitive information can be originated by CSEA personnel during the course of an inquiry or investigation or it can be received and transmitted to and from other law enforcement agencies or organizations. Law Enforcement Sensitive information, by definition, is exempt from Freedom of Information Act disclosure.

Designating authority: Deputy Associate Director of the Center for Security and Emergency Actions (CSEA).

Policies or procedures for specialized training for designators: No

Systematic review process: No

Designation: Critical Infrastructure Information

Basis for designation: Not specified

Definition: The term used within OPM to protect voluntarily shared information from public disclosure: financial services, telecommunications, transportation, energy, emergency services, and government essential services, whose disruption or destruction would affect our economic or national security.

Designating authority: Deputy Associate Director of the Center for Security and Emergency Actions (CSEA).

Policies or procedures for specialized training For designators: No

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Small Business Administration

Agencywide

Designation: None

Basis for designation: (new policy in draft)

Definition: N/A

Designating authority: N/A

**Policies or procedures for specialized training for
designators:** N/A

Systematic review process: N/A

Social Security Administration

Agencywide

Designation: Official Use Only

Basis for designation: Union/Management Agreement (October 1997) and SSA Administrative Instruction Manual (February 2003)

Definition: The designation was agreed to by SSA management and the union on the distribution, review, and maintenance of physical security survey reports. The designation is to limit access to the reports to authorized personnel who have a need to know the details of contractor-produced physical security facility reviews for the purpose of reviewing recommendations and taking corrective actions.

Designating authority: N/A

Policies or procedures for specialized training for designators: N/A

Systematic review process: N/A

Office of Income Security Programs

Designation: Sensitive Instructions

Basis for designation: Policy Writer's Toolkit (April 2005)

Definition: Sensitive Instructions are intranet policy or processing instructions available to SSA personal but not available to the public.

Designating authority: Decided by author of the policy or system instruction based on guidance provided in the Toolkit.

Policies or procedures for specialized training for designators: No

Systematic review process: No

Office of Policy

Designation: Confidential Information Protection and Statistical Efficiency Act

Basis For designation: Confidential Information Protection and Statistical Efficiency Act (Title V of Pub. L. No. 107-347, see 44 U.S.C. § 3501, note)

Definition: Data or information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes. The information is to be used by officers, employees, or agents of the agency exclusively for statistical purposes.

Designating authority: The Associate Commissioner of the Office of Research, Evaluation, and Statistics is authorized to make this designation for the Office of Policy.

Policies or procedures for specialized training for designators: N/A

Systematic review process: No

**Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency**

Office of Realty and Management

Designation: For Official Use Only

Basis for designation: GSA Order, PBS 3490.1 (March 2002)—GSA policy for federal buildings

Definition: All building information falls under the designation. The designation remains in force for the entire life cycle of a building, from design inception through construction, and to the demolition or lease termination for the property.

Designating authority: Not specified.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

United States Agency for International Development
Agencywide

Designation: Sensitive But Unclassified

Basis for designation: State Department's 12 FAM 540 and Automated Directive System 568.3.2

Definition: The designation is used for official information and material that is not national security information, and therefore is not classifiable, but nevertheless requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of the agency to accomplish its mission, proprietary data, records requiring protection under the Privacy Act and data not releasable under the Privacy Act and the Freedom of Information Act (5 U.S.C. § 552).

Designating authority: Any official having management authority for the information.

**Policies or procedures for specialized training for
designators:** No

Systematic review process: No

Appendix II: Summary Information on
Sensitive But Unclassified Designations by
Agency

United States Postal Service

Agencywide

Designation: Sensitive Information

Basis for designation: 39 C.F.R. § 262.3(a)

Definition: Information that has been identified by the USPS as restricted or critical.

Designating authority: Chief Privacy Officer and Corporate Information Security Officer.

**Policies or procedures for specialized training for
designators:** Yes

Systematic review process: Yes

Appendix III: Comments from the Office of the Director of National Intelligence

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

March 2, 2006

Henry L. Hinton, Jr.
Managing Director, Defense Capabilities and Management
United States Government Accountability Office
Washington, D.C. 20548

Dear Mr. Hinton:

We appreciate the opportunity to review the Government Accountability Office's (GAO) March 2006 draft report entitled, *The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, as conveyed in your February 9, 2006 letter.

The draft report is very broad and addresses a number of intelligence-related issues, including a discussion of the management of the Office of the Director of National Intelligence (ODNI) and specific recommendations to the Director of National Intelligence (DNI).

We are aware that you have been previously advised by the Department of Justice that the review of intelligence activities is beyond the GAO's purview. For similar reasons, we decline to provide the GAO with comments on the draft report.

The Congress and the Executive Branch have established a long-standing, effective and efficient process for the oversight of intelligence activities. To assist Congress in its oversight responsibilities, the Executive Branch regularly provides information and briefings to the congressional intelligence committees, and to other committees of jurisdiction, on relevant topics including information sharing within the Federal government and the activities of the Program Manager for the Information Sharing Environment.

If you have any questions concerning this matter, please contact Mr. Peter Petrihos, in the Office of Legislative Affairs, at 703-482-5616.

Sincerely,



Kathleen Turner
Deputy Director
Office of Legislative Affairs

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

David Powner at (202) 512-9286 or pownerd@gao.gov or Eileen Larence at (202) 512-6510 or larencee@gao.gov

Staff Acknowledgments

In addition to the individual named above, Susan Quinlan, Assistant Director, Rochelle Burns, Joanne Fiorino, Thomas Lombardi, Lori Martinez, Vickie Miller, David Plocher, John Stradling, Morgan Walts, and Marcia Washington made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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