United States Government Accountability Office

GAO

Report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

May 2008

PRIVACY

Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions

GAO-08-603

May 2008

PRIVACY

Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-603, a report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Government agencies have a long-standing obligation under the Privacy Act of 1974 to protect the privacy of individuals about whom they collect personal information. A number of additional laws have been enacted in recent years directing agency heads to designate senior officials as focal points with overall responsibility for privacy.

GAO was asked to (1) describe laws and guidance that set requirements for senior privacy officials within federal agencies, and (2) describe the organizational structures used by agencies to address privacy requirements and assess whether senior officials have oversight over key functions. To achieve these objectives, GAO analyzed the laws and related guidance and analyzed policies and procedures relating to key privacy functions at 12 agencies.

What GAO Recommends

GAO is recommending that certain agencies it reviewed take steps to ensure that their senior agency officials for privacy have oversight of all key privacy functions. Seven of the 12 agencies had no comment or concurred with GAO's assessment. Commerce and Defense did not state whether they agreed, but said that their current structures were adequate. Justice, Labor, and Treasury disagreed with GAO's characterization of their senior privacy officials as not having oversight of all key privacy functions. However, these agencies' policies do not assign oversight of such functions to their senior privacy officials.

To view the full product, including the scope and methodology, click on GAO-08-603. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Federal laws set varying roles and responsibilities for senior agency privacy officials. Despite much variation, all of these laws require covered agencies to assign overall responsibility for privacy protection and compliance to a senior agency official. In addition, Office of Management and Budget guidance directs agencies to designate a senior agency official for privacy with specific responsibilities. The specific privacy responsibilities defined in these laws and guidance can be grouped into six broad categories: (1) conducting privacy impact assessments (which are intended to ensure that privacy requirements are addressed when personal information is collected, stored, shared, and managed in a federal system), (2) complying with the Privacy Act, (3) reviewing and evaluating the privacy implications of agency policies, (4) producing reports on the status of privacy protections, (5) ensuring that redress procedures to handle privacy inquiries and complaints are in place, and (6) ensuring that employees and contractors receive appropriate training. The laws and guidance vary in how they frame requirements in these categories and which agencies must adhere to them.

Agencies also have varying organizational structures to address privacy responsibilities. For example, of the 12 agencies we reviewed, 2 had statutorily designated chief privacy officers who also served as senior agency officials for privacy, 5 designated their agency chief information officers as their senior privacy officials, and the others designated a variety of other officials, such as the general counsel or assistant secretary for management. Further, not all of the agencies we reviewed had given their designated senior officials full oversight over all privacy-related functions. While 6 agencies had these officials overseeing all key privacy functions, 6 others relied on other organizational units not overseen by the designated senior official to perform certain key privacy functions. The fragmented way in which privacy functions were assigned to organizational units in these agencies is at least partly the result of evolving requirements in law and guidance. However, without oversight of all key privacy functions, designated senior officials may be unable to effectively serve as agency central focal points for information privacy.

Contents

Figures

Abbreviations

CIO	chief information officer
CPO	chief privacy officer
CISO	chief information security officer
DHS	Department of Homeland Security
E-Gov Act	E-Government Act
FISMA	Federal Information Security Management Act
OMB	Office of Management and Budget
PIA	privacy impact assessment
SAOP	senior agency official for privacy

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 30, 2008

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Senator Akaka:

As you know, government agencies have long-standing obligations to protect the privacy of individuals about whom they collect personal information. Based on concerns about privacy, a number of laws have been enacted in recent years directing agency heads to designate chief privacy officers (CPO) as focal points with overall responsibility for privacy. For example, the Homeland Security Act of 2002 created the first statutorily required senior privacy official at the Department of Homeland Security (DHS). Several other laws followed with similar direction to other agencies. Furthermore, the Office of Management and Budget (OMB) issued guidance in 2005 directing each agency to designate a senior agency official for privacy (SAOP).

Agency responsibilities for protecting privacy are based primarily on two laws, the Privacy Act of 1974 and the E-Government Act (E-Gov Act) of 2002. Under the Privacy Act, federal agencies must issue public notices that identify, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information. The E-Gov Act requires agencies to conduct privacy impact assessments (PIA) of privacy risks associated with information technology used to process personal information.[1] In addition, the Paperwork Reduction Act sets conditions for collecting information from individuals and designates agency chief information officers (CIO) as responsible for privacy protection. Recent laws and guidance have also

[1]A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system to ensure that privacy requirements are addressed.

designated specific agency officials with responsibilities for ensuring agency compliance with privacy protection requirements.

Our objectives were to (1) describe laws and guidance that set requirements for senior privacy officials within federal agencies, and (2) describe the organizational structures used by agencies to address privacy requirements and assess whether senior officials have oversight over key functions.

To address our first objective, we reviewed and analyzed laws and OMB guidance that assign agencywide privacy responsibilities to senior officials within federal agencies. To address our second objective, we analyzed policies and procedures at these agencies, and interviewed senior agency privacy officials to identify the privacy management structures used at each of these agencies and the roles and responsibilities of senior privacy officials. The agencies included in this review (Departments of Commerce, Defense, Health and Human Services, Homeland Security, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs, as well as the Social Security Administration and the U.S. Agency for International Development) are major agencies with statutorily designated privacy officers, have a central mission for which the collection of personally identifiable information is a critical component, or have implemented a unique organizational privacy structure. We examined and compared agency management structures for fulfilling privacy responsibilities and assessed the differences in roles and responsibilities of privacy officers based on the differences in agencies' organizational structures. We conducted this performance audit from September 2007 to May 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Laws and guidance set a variety of requirements for senior privacy officials at federal agencies. For example, agencies have had a long standing requirement under the Paperwork Reduction Act to assign agency CIOs overall responsibility for privacy policy and compliance with the Privacy Act. In recent years, additional laws have also set roles and responsibilities for senior agency privacy officials. Despite much variation, all of these laws require agencies to assign overall responsibility for privacy protection and compliance to a senior official. In addition, OMB

guidance directs agencies to designate an SAOP with specific responsibilities. These laws and guidance define specific privacy responsibilities that can be grouped into six broad categories: (1) conducting PIAs; (2) complying with the Privacy Act; (3) reviewing and evaluating the privacy implications of agency policies, regulations, and initiatives; (4) producing reports on the status of privacy protections; (5) ensuring that redress procedures are in place; and (6) ensuring that employees and contractors receive appropriate training. The laws and guidance vary in how they frame requirements in these categories and which agencies must adhere to them.

Agencies have varying organizational structures to address privacy responsibilities. For example, of the 12 agencies we reviewed, 2 had statutorily designated CPOs who also served as SAOPs, 5 designated their agency CIOs as their senior officials, and the others designated a variety of other officials, such as the general counsel or assistant secretary for management. Further, not all of the agencies we reviewed had given their designated senior officials full oversight over all privacy-related functions. While 6 agencies had these officials overseeing all key privacy functions, 6 others relied on other organizational units not overseen by the designated senior official to perform certain key privacy functions. The fragmented way in which privacy functions have been assigned to organizational units in these agencies is at least partly the result of evolving requirements in law and guidance. As requirements have evolved, organizational responsibilities have been established incrementally to meet them. However, without oversight and involvement in all key privacy functions, SAOPs may be unable to effectively serve as agency central focal points for information privacy.

We are recommending that the heads of certain agencies we reviewed take steps to ensure that their SAOPs have oversight over all key privacy functions.

We provided a draft of this report to OMB and to the Departments of Commerce, Defense, Health and Human Services, Homeland Security, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs, as well as the Social Security Administration and the U.S. Agency for International Development, for review and comment. Five agencies provided no comments on this review.[2] In comments provided via Email,

[2]These agencies are Health and Human Services, Homeland Security, State, Transportation, and the U.S. Agency for International Development.

the Veterans Affairs and the Social Security Administration concurred with our assessment and recommendations and provided technical comments, which we incorporated in the final report as appropriate. In oral comments, OMB also concurred with our assessment and recommendations and provided technical comments, which we incorporated in the final report as appropriate. Commerce and Defense provided written comments that did not state whether they agreed or disagreed with the content of the report; however, both agencies stated that their privacy management structures were adequate. In contrast, we believe that clearly establishing the role of the SAOP as a focal point for departmental privacy functions would help ensure that these agencies provide consistent privacy protections and would align with OMB direction. Justice, Labor, and Treasury provided written comments and disagreed with our characterization of their agency SAOPs as not having oversight of all key privacy functions. However, our review of agency policies and procedures relating to privacy management showed that SAOPs at these agencies had not been assigned oversight of all key functions.

Background

In recent years, a number of factors have led to growing concern about the protection of privacy when personally identifiable information is collected and maintained by the federal government.[3] Recent data breaches of personal information at government agencies, such as the data breach at the Department of Veterans Affairs, which exposed the personal information of 26.5 million veterans and active duty members of the military in May 2006, have raised concerns about identity theft.[4] In addition, increasingly sophisticated analytical techniques employed by federal agencies, such as data mining, also raise concerns about how personally identifiable information is used and what controls are placed

[3]For purposes of this report, the terms *personal information* and *personally identifiable information* are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records, and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[4]For analysis of issues associated with the Veterans Affairs data breach, see GAO, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information*, GAO-06-833T (Washington, D.C.: June 8, 2006) and *Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues*, GAO-06-866T (Washington, D.C.: June 14, 2006).

on its use. Concerns such as these have focused attention on the structures agencies have instituted to ensure privacy protections are in place.

The major requirements for privacy protection by federal agencies come from two laws, the Privacy Act of 1974 and the E-Gov Act of 2002.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies maintain a system of records, they must notify the public by a system-of-records notice: that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" use of the data, and procedures that individuals can use to review and correct personal information. The act also requires agencies to define and limit their use of covered personal information. In addition, the act requires that to the greatest extent practicable, personal information should be collected directly from the subject individual when it may affect an individual's rights or benefits under a federal program.

The E-Gov Act of 2002 also assigns agencies significant responsibilities relating to privacy. The E-Gov Act strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct PIAs. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Furthermore, according to OMB guidance, a PIA is an analysis of how information is handled. Specifically, a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form or (2) before initiating

any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available, they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

OMB is tasked with providing guidance to agencies on how to implement the provisions of these two acts and has done so, beginning with guidance on the Privacy Act, issued in 1975. The guidance provides explanations for the various provisions of the law as well as detailed instructions on how to comply. OMB's guidance on implementing the privacy provisions of the E-Gov Act of 2002 identifies circumstances under which agencies must conduct PIAs and explains how to conduct them.

We have previously reported on the role of senior privacy officials in the federal government. In 2006, we testified that the elevation of privacy officers to senior positions reflected the growing demands that these individuals faced in addressing privacy challenges on a day-to-day basis.[5] The challenges we identified included ensuring compliance with relevant privacy laws, such as the Privacy Act and the E-Gov Act, and controlling the collection and use of personal information obtained from commercial sources. Additionally, in 2007 we reported that the DHS Privacy Office had made significant progress in carrying out its statutory responsibilities under the Homeland Security Act and its related role in ensuring E-Gov Act compliance, but noted that more work remained to be accomplished.[6] We recommended that DHS designate privacy officers at key DHS components, implement a department wide process for reviewing Privacy Act notices, establish a schedule for the timely issuance of privacy reports, and ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations. In response, DHS included a discussion of privacy complaints in its most recent annual report; however, the other recommendations have not yet been implemented.

[5]GAO, *Privacy: Key Challenges Facing Federal Agencies*, GAO-06-777T (Washington, D.C.: May 17, 2006).

[6]GAO, *DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public*, GAO-07-522 (Washington, D.C.: Apr 27, 2007).

Laws and Guidance Set Varying Requirements for Senior Privacy Officials

Laws and guidance set a variety of requirements for senior privacy officials at federal agencies. For example, agencies have had a long standing requirement under the Paperwork Reduction Act to assign agency CIOs overall responsibility for privacy policy and compliance with the Privacy Act. In recent years, additional laws have been enacted that also address the roles and responsibilities of senior officials with regard to privacy. Despite much variation, all of these laws require agencies to assign overall responsibility for privacy protection and compliance to a senior agency official. In addition, OMB guidance has directed agencies to designate senior officials with overall responsibility for privacy.

These laws and guidance set specific privacy responsibilities for these agency officials. These responsibilities can be grouped into six broad categories: (1) conducting PIAs; (2) Privacy Act compliance; (3) reviewing and evaluating the privacy implications of agency policies, regulations, and initiatives; (4) producing reports on the status of privacy protections; (5) ensuring that redress procedures are in place; and (6) ensuring that employees and contractors receive appropriate training. The laws and guidance vary in how they frame requirements in these categories and which agencies must adhere to them.

Laws and Guidance Address the Roles and Responsibilities of Privacy Officials

Numerous laws assign privacy responsibility to senior agency officials. The earliest of these laws is the Paperwork Reduction Act of 1980, which, as amended, directs agency heads to assign a CIO with responsibility for carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness.[7] The act directs agency CIOs to undertake responsibility for implementing and enforcing applicable privacy policies, procedures, standards, and guidelines, and to assume responsibility and accountability for compliance with and coordinated management of the Privacy Act of 1974 and related information management laws.[8]

[7]While the Privacy Act of 1974 established privacy responsibilities for agencies, it did not specify a senior agency official to be responsible for meeting these requirements.

[8]OMB issued guidance for agencies on the implementation of the Paperwork Reduction Act, including the responsibility of CIOs for privacy. See OMB Circular A-130, *Management of Federal Information Resources* (Washington D.C.: November 28, 2000). For an analysis of CIO roles and responsibilities, see GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

As concerns about privacy have increased in recent years, Congress has enacted additional laws that include provisions addressing the roles and responsibilities of senior officials with regard to privacy. Despite variations, a common thread among these laws, as well as relevant OMB guidance, is that they all require agencies to assign overall responsibility for privacy protection and compliance to a senior agency official. Relevant laws include the following:

- The Homeland Security Act of 2002 directed the secretary of DHS to designate a senior official with primary responsibility for privacy policy.
- The Intelligence Reform and Terrorism Prevention Act of 2004 required the Director of National Intelligence to appoint a Civil Liberties Protection Officer and assigned this individual specific privacy responsibilities.
- The Violence Against Women and Department of Justice Reauthorization Act of 2005 instructed the Attorney General to designate a senior official with primary responsibility for privacy policy.
- The Transportation, Treasury, Independent Agencies and General Government Appropriations Act of 2005 directed each agency whose appropriations were provided by the act, including the Departments of Transportation and Treasury, to designate a CPO with primary responsibility for privacy and data protection policy.[9]
- The Implementing Recommendations of the 9/11 Commission Act of 2007 instructed the heads of Defense, DHS, Justice, Treasury, Health and Human Services, and State, as well as the Office of the Director of

[9]The Transportation, Treasury, Independent Agencies and General Government Appropriations Act of 2005 applies to the Department of Transportation, Department of Treasury, Executive Office of the President, Architectural and Transportation Barriers Compliance Board, Election Assistance Commission, Federal Election Commission, Federal Labor Relations Authority, Federal Maritime Commission, General Services Administration, Merit Systems Protection Board, Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation, National Archives and Records Administration, National Historical Publications and Records Commission, National Transportation Safety Board, Office of Government Ethics, Office of Personnel Management, Office of Special Counsel, U.S. Postal Service, and U.S. Tax Court.

National Intelligence and the Central Intelligence Agency to designate no less than one senior officer to serve as a privacy and civil liberties officer.[10] Specific privacy provisions of these laws are summarized in appendix II.

A number of OMB memorandums have also addressed the roles and responsibilities of senior privacy officials. In 1999, OMB required agencies to designate a senior official to assume primary responsibility for privacy policy.[11] OMB later reiterated this requirement in its guidance on compliance with the E-Gov Act, in which it directed agency heads to designate an appropriate senior official with responsibility for the coordination and implementation of OMB Web and privacy policy and to serve as the agency's principal contact for privacy policies.[12] Most recently, in 2005, OMB directed agencies to designate an SAOP with agency wide responsibility for information privacy issues and with responsibility for specific privacy functions, including ensuring agency compliance with all federal privacy laws, playing a central policy-making role in the development of policy proposals that implicate privacy issues, and ensuring that contractors and employees are provided with adequate privacy training.[13]

Beginning in 2005, OMB has also issued guidance significantly enhancing longstanding requirements for agencies to report on their compliance with privacy laws.[14] OMB's 2005 guidance directed agencies to add a new section addressing privacy to their annual reports under the Federal Information Security Management Act (FISMA).[15] SAOPs were assigned

[10]This law grants the Privacy and Civil Liberties Oversight Board authority to require any other agency or element of the executive branch to establish a privacy and civil liberties officer. Further, this law specifies that if covered agencies have another statutorily designated privacy officer, this officer must also undertake the responsibilities described in the act.

[11]Office of Management and Budget, *OMB Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"*, M-99-05 (Washington, D.C.: Jan. 7, 1999).

[12]Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

[13]Office of Management and Budget, *Designation of Senior Agency Officials for Privacy*, M-05-08 (Feb. 11, 2005).

[14]Office of Management and Budget, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-05-15 (Washington, D.C.: June 13, 2005).

[15]FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

responsibility for completion of this section, in which they were to report on such things as agency policies and procedures for the conduct of PIAs, agency policies for ensuring adequate privacy training, as well as their own involvement in agency regulatory and policy decisions. In 2006, OMB issued further guidance requiring agencies to include as part of their FISMA reports a section addressing measures for protecting personally identifiable information. This guidance also required that agencies provide OMB with quarterly privacy updates and report all incidents relating to the loss of or unauthorized access to personally identifiable information.[16] Most recently, OMB directed agencies in 2007 to include in their FISMA reports additional items, such as their breach notification policies, plans to eliminate unnecessary use of Social Security numbers, and plans for reviewing and reducing their holdings of personally identifiable information.[17]

These laws and guidance set a variety of requirements for senior officials to carry out specific privacy responsibilities. These responsibilities can be grouped into the following six key functions:

- *Conduct of PIAs:* A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system, and is required before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form. Several laws assign privacy officials at covered agencies responsibilities that are met in part by performing PIAs on systems that collect, process, or store personally identifiable information. This includes the requirements for several agencies to ensure that "technologies sustain and do not erode privacy protections." Furthermore, OMB guidance requires agency SAOPs to ensure compliance with federal laws, regulations, and policies relating to information privacy, such as the E-Gov Act, which spells out agency PIA requirements.

- *Privacy Act compliance:* As previously discussed, the Privacy Act sets a variety of requirements for all federal agencies regarding privacy protection. For example, the act requires that when agencies establish or

[16]Office of Management and Budget, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-06-20 (Washington, D.C.: July 17, 2006).

[17]Office of Management and Budget, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, ,M-07-19 (Washington, D.C.: July 25, 2007).

make changes to a system of records, they must notify the public by a notice in the Federal Register , identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" use of the data, and procedures that individuals can use to review and correct personal information. Several other laws explicitly direct agency privacy officials to ensure that the personal information contained in their Privacy Act systems of records is handled in compliance with fair information practices as set out in the act. Further, OMB guidance assigns agency SAOPs with responsibility for ensuring Privacy Act compliance.

- *Policy consultation:* Relevant laws direct senior privacy officials to actively participate in the development and evaluation of privacy-sensitive agency policy decisions. Several specifically task the SAOP with evaluating legislative and regulatory proposals or periodically reviewing agency actions affecting privacy. As agencies develop new policies, senior officials responsible for privacy issues play a key role in identifying and mitigating potential privacy risks prior to finalizing a particular policy decision. Moreover, OMB directed agency SAOPs to undertake a central role in the development of policy proposals that implicate privacy issues.

- *Privacy reporting:* Agency senior privacy officials are often required to prepare periodic reports to ensure transparency about their activities and compliance with the law. Many laws reviewed required agencies to produce periodic privacy reports to agency stakeholders and Congress. OMB also requires agency SAOPs to report on their privacy activities as part of their annual FISMA reports, including such measures as their total numbers of systems of records, the number of written privacy complaints they have received, and whether a senior official has responsibility for all privacy-related activities.

- *Redress:* With regard to federal agencies, the term "redress" generally refers to an agency's complaint resolution process, whereby individuals may seek resolution of their concerns about an agency action. Specifically, in the privacy context, redress refers to processes for handling privacy inquiries and complaints as well as for allowing citizens who believe that agencies are storing and using incorrect information about them to gain access to and correct that information. The Privacy Act requires that all agencies, with certain exceptions, allow individuals access to their records and the ability to have inaccurate information corrected. Several recent laws also direct senior privacy officials at specific agencies to provide redress by ensuring that they have adequate procedures for investigating and addressing privacy complaints by individuals. Several laws also

provide for attention to privacy in a broader context of civil liberties protection.

- *Privacy training:* Privacy training is critical to ensuring that agency employees and contractor personnel follow appropriate procedures and take proper precautions when handling personally identifiable information. For example, The Transportation, Treasury, Independent Agencies and General Appropriations Act of 2005 requires senior privacy officials at covered agencies to ensure that employees have adequate privacy training. OMB also requires agency SAOPs to ensure that employees and contractors receive privacy training.

In addition to performing key privacy functions, requirements in laws include responsibilities to ensure adequate security safeguards to protect against unauthorized access, use, disclosure, and destruction of sensitive personal information. Generally, this is provided through agency information security programs established under FISMA, and overseen by agency CIOs and chief information security officers (CISO).[18] Moreover, OMB has issued guidance instructing agency heads to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.

Figure 1 shows the extent to which laws have requirements that specifically address each privacy function and to which agencies these requirements apply.[19]

[18]For purposes of this report, we did not address information security assurance as a privacy function. Prior GAO reports have examined information security at federal agencies. For example, in March 2008, we testified that agencies continue to experience significant information security control deficiencies and that most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. As a result, federal systems and information were at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information. See GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: Mar. 12, 2008).

[19]These laws may make designated agency officials responsible for additional privacy functions that are not specifically mentioned. For example, by designating agency officials as responsible for Privacy Act compliance, these laws would implicitly make such officials responsible for meeting all requirements specified in the Privacy Act, including such things as providing a means to access and correct information, which is a component of the redress function.

Figure 1: Laws with Provisions That Specifically Address Key Privacy Functions

Laws and guidance	Apply to	Privacy functions: PIA	Privacy Act compliance	Policy consultation	Reporting	Redress	Training
Homeland Security Act of 2002	DHS	●	●	●	●		
Intelligence Reform and Terrorism Prevention Act of 2004	Office of the Director of National Intelligence	●	●	●		●	
Violence Against Women and Department of Justice Reauthorization Act of 2005	Department of Justice	●	●	●	●	●	●
Transportation, Treasury, Independent Agencies and General Government Appropriations Act of 2005	All entities whose appropriations are provided by this act. This includes Transportation, Treasury and many other entities.	●	●	●	●		●
Implementing Recommendations of the 9/11 Commission Act of 2007[a]	Department of Defense, DHS, Justice, Treasury, Health and Human Services, State, Office of the Director of National Intelligence, and the Central Intelligence Agency			●	●	●	
OMB memo M-05-08: *Designation of Senior Agency Officials for Privacy*	All executive branch agencies	●	●	●			●
OMB memos M-06-20, M-07-19, M-08-09	All executive branch agencies				●		

● Provision relating to key function

No provision

Source: GAO analysis.

[a]This act also contains more specific requirements for DHS regarding PIAs, Privacy Act compliance, and training.

Agencies Have Varying Privacy Management Structures, and Senior Agency Officials for Privacy Do Not Consistently Have Oversight of All Key Functions

Agencies have varying organizational structures to address privacy responsibilities. For example, of the 12 agencies we reviewed, 2 had statutorily designated CPOs who also served as SAOPs, 5 designated their agency CIOs as their senior officials, and the others designated a variety of other officials, such as the general counsel or assistant secretary for management. Further, not all of the agencies we reviewed had given their designated senior officials full oversight over all privacy-related functions. While 6 agencies had these officials overseeing all key privacy functions, 6 others relied on other organizational units not overseen by the designated senior official to perform certain key privacy functions. The fragmented way in which privacy functions have been assigned to organizational units in these agencies is at least partly the result of evolving requirements in law and guidance. As requirements have evolved, organizational responsibilities have been established incrementally to meet them.

However, without oversight and involvement in all key privacy functions, SAOPs may be unable to effectively serve as agency central focal points for privacy.

Agencies Varied in Their Designation of Senior Privacy Officials and in Their Organizational Placement of Key Privacy Functions

Agencies have taken varied approaches to designating senior agency officials with privacy responsibilities. Two of the 12 agencies we reviewed had separate CPOs that were also designated as the senior officials for privacy. Five agencies assigned their agency CIOs as SAOPs, and 1 agency assigned its CISO. Lastly, 4 agencies assigned another high-level official, such as a general counsel or assistant secretary for management, as the SAOP.

In addition to varying in how they designated senior officials for privacy, agencies also varied in the way they assigned privacy responsibilities to organizational units. Four of the 12 agencies we reviewed (Transportation, DHS, State, and U.S. Agency for International Development) had one organization primarily responsible for all of the six key privacy functions outlined in the previous section. The remaining 8 agencies (Social Security Administration, Veterans Affairs, Defense, Commerce, Labor, Justice, Treasury, and Health and Human Services) relied on more than one organizational unit to perform privacy functions. Figure 2 summarizes the organizational structures in place at agencies to address the six key privacy functions, including the specific organizational units responsible for carrying out each of the key privacy functions.

Figure 2: Responsibility for Key Privacy Functions at 12 Agencies

Agency	SAOP	Privacy functions					
		PIA	Privacy Act compliance	Policy Consultation	Redress	Reporting	Training
Department of Transportaion	CIO	Office of the CIO / Office of the General Counsel	Office of the CIO / Office of the General Counsel	Office of the CIO	Office of the CIO	Office of the CIO	Office of the CIO
DHS	Chief Privacy Officer	Privacy Office	Privacy Office	Privacy Office	Privacy Office	Privacy Office	Privacy Office
Social Security Administration	General Counsel	Office of Public Disclosure	Office of Public Disclosure	Office of Public Disclosure	Office of General Law / Office of Public Disclosure	Office of Public Disclosure	Office of Public Disclosure
State	Assistant Secretary for Administration	Office of Information Programs and Services	Office of Information Programs and Services	Office of Information Programs and Services	Office of Information Programs and Services	Office of Information Programs and Services	Office of Information Programs and Services
U. S. Agency for International Development	Chief Privacy Officer	Privacy Office	Privacy Office	Privacy Office	Privacy Office	Privacy Office	Privacy Office
Veterans Affairs	CIO	Privacy Service	Records Management Service	Privacy Service	Privacy Service / Components	Privacy Service	Privacy Service
Department of Justice	Chief Privacy and Civil Liberties Officer	Privacy and Civil Liberties Office	Privacy and Civil Liberties Office	Privacy and Civil Liberties Office	Components	Privacy and Civil Liberties Office	Privacy and Civil Liberties Office
Treasury	Assistant Secretary for Management	Office of the CIO / Components	Office of the Deputy Assistant Secretary for Headquarters Operations	Office of the Deputy Assistant Secretary for Headquarters Operations / Office of the CIO	Components	Office of the Deputy Assistant Secretary for Headquarters Operations / Office of the CIO	Office of the Deputy Assistant Secretary for Headquarters Operations / Components
Department of Commerce	CIO	Office of the CIO	Privacy Act Office	Office of the CIO/ Office of the General Counsel	Privacy Act Office	Office of the CIO/ Privacy Act Office	Office of the CIO
Department of Defense	Director for Administration and Management	Office of the CIO	Defense Privacy Office	Defense Privacy Office	Components	Defense Privacy Office	Defense Privacy Office
Department of Labor	CIO	Office of the CIO	Office of the Solicitor	Office of the CIO	Office of the Solicitor	Office of the CIO	Office of the Solicitor
Health and Human Services	CIO	Office of the CIO	Privacy Act Officer	Senior Advisor, Privacy Policy	Privacy Act Officer	Office of the CIO / Components	Office of the CIO

Overseen by the agency SAOP

Not overseen by the agency SAOP

Source: GAO analysis of agency data.

Six of the agencies (DHS, State, Social Security Administration, Transportation, U.S. Agency for International Development, and Veterans Affairs) established privacy structures in which the SAOP oversaw all key privacy functions. For example, DHS's Privacy Office performed these

functions under the direction of the CPO, who was also the department's SAOP. Similarly, U.S. Agency for International Development's CISO (also the SAOP) oversaw the agency's privacy office, which was responsible for all key functions. While more than one organizational unit carried out privacy functions in two cases (Veterans Affairs and the Social Security Administration), all such units were overseen by the senior agency official for privacy.

However, six other agencies (Commerce, Health and Human Services, Labor, Transportation, Defense, and Treasury) had privacy management structures in which the SAOP did not oversee all key privacy functions. For two agencies—Justice and Treasury—the SAOP had oversight over all key functions except for redress, which was handled by individual component organizations. For the other four agencies, key functions were divided among two or more organizations, and the senior privacy official did not have oversight of all of them. For example, key privacy functions at Labor were being performed not only by the office of the CIO (who is also the SAOP) but also by the Office of the Solicitor, who is independent of the CIO. Likewise, the senior official at Commerce was responsible for overseeing conduct of PIAs, policy consultation, and privacy training, while a separate Privacy Act Officer was responsible for Privacy Act compliance. Without full oversight of key privacy functions, SAOPs may be limited in their ability to ensure that privacy protections are administered consistently across the organization.

Evolving Requirements in Laws and Related Guidance Have Led to Fragmented Assignment of Privacy Functions

The fragmented way in which privacy functions have been assigned to organizational units in several agencies is at least partly the result of evolving requirements in law and guidance. As requirements have evolved, organizational responsibilities have been established incrementally to meet them. For example, although the Privacy Act does not specify organizational structures for carrying out its provisions, many agencies established Privacy Act officers to address the requirements of that act and have had such positions in place for many years. In some cases, agencies designated their general counsels to be in charge of ensuring that the Privacy Act's requirements were met. More recently, the responsibility to conduct PIAs under the E-Gov Act frequently has been given to another office, such as the Office of the CIO, because the E-Gov Act's requirements apply to information technology, which is generally the purview of the CIO. If an SAOP was designated in such agencies without reassigning these responsibilities, that official may not have oversight and involvement in all key privacy activities.

Uneven implementation of the Paperwork Reduction Act also may have contributed to fragmentation of privacy functions. As previously discussed, the Paperwork Reduction Act requires agency CIOs to take responsibility for privacy policy and compliance with the Privacy Act, and thus agencies could ensure they are in compliance with the Paperwork Reduction Act by designating their CIOs as SAOPs.[20] However, 7 out of the 12 agencies we reviewed did not designate their CIOs as SAOPs. Further, if CIOs were designated as agency SAOPs but did not have responsibility for compliance with the Privacy Act—as was the case at Commerce, Labor, and Health and Human Services—the SAOPs would be left without full oversight of key privacy functions.

Agencies that have more than one internal organization carrying out privacy functions run the risk that those organizations may not always provide the same protections for personal information if they are not overseen by a central authority. Thus, unless steps are taken to ensure that key privacy functions are under the oversight of the SAOP, agencies may be limited in their ability to ensure that information privacy protections are implemented consistently across their organizations.

Conclusions

While agencies have had the responsibility for many years to establish management structures to ensure coordinated implementation of privacy policy and compliance with the Privacy Act, recent laws and guidance have significantly changed requirements for privacy oversight and management. These laws and guidance vary in scope and specificity, but they all require the designation of a senior agency official with overall responsibility for privacy protection and compliance with statutory requirements.

In adopting varied assignments for key privacy functions, not all agencies gave their SAOPs responsibility for all key privacy functions. As a result, agencies may not be implementing privacy protections consistently. While the particulars of privacy management may vary according to the size of

[20]In 2004, GAO reported that 17 of 27 CIOs were responsible for privacy, See GAO-04-823. OMB guidance also acknowledged the Paperwork Reduction Act's CIO requirement, but stated that the CIO "may perform" the privacy role, and that "if the CIO, for some reason, is not designated, the agency may have designated another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues. In any case, the senior agency official should have authority within the agency to consider information privacy policy issues at a national and agency-wide level." M-05-08 (Feb. 11, 2005).

the agency and the sensitivity of its mission, agencies generally would likely benefit from having SAOPs that serve as central focal points for privacy matters and have oversight of all key functions, as required by law and guidance. Such focal points can help ensure that agency activities provide consistent privacy protections.

Recommendation for Executive Action

In order to ensure that their SAOPs function effectively as central focal points for privacy management, we recommend that the Attorney General and the Secretaries of Commerce, Defense, Health and Human Services, Labor, and Treasury take steps to ensure that their SAOPs have oversight over all key privacy functions.

Agency Comments and Our Evaluation

We provided a draft of this report to OMB and to the departments and agencies we reviewed: the Departments of Commerce, Defense, Health and Human Services, Homeland Security, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs, as well as the Social Security Administration and the U.S. Agency for International Development, for review and comment. Five agencies provided no comments on this draft.[21] In comments provided via email, the Associate Deputy Assistant Secretary for Privacy and Records Management at Veterans Affairs and the Audit Management Liaison at the Social Security Administration concurred with our assessment and recommendations and provided technical comments, which we incorporated in the final report as appropriate. In oral comments, the Acting Branch Chief of the Information Policy and Technology Branch at OMB also concurred with our assessment and recommendations and provided technical comments, which we incorporated in the final report as appropriate. Commerce and Defense provided written comments that did not state whether they agreed or disagreed with our recommendations; however, both agencies stated that their privacy management structures were adequate. Their comments are reprinted in appendixes II and III respectively. Justice, Labor, and Treasury provided written comments and disagreed with our characterization of their agency SAOPs as not having oversight of all key privacy functions. Their comments are reprinted in appendixes IV, V, and VI respectively.

[21]These agencies are Health and Human Services, Homeland Security, State, Transportation, and the U.S. Agency for International Development.

The Chief Information Officer of the Department of Commerce stated that the department agreed with our characterization of the fragmentation that has resulted from recent laws and guidance that have significantly changed requirements for privacy oversight and management. However, she stated that applicable law does not require that the administration of the Privacy Act be consolidated with other privacy functions under the Office of the Chief Information Officer. Law and OMB guidance direct agencies to have a senior agency official, the CIO in the case of the Paperwork Reduction Act, serving as a focal point for privacy and ensuring compliance with the Privacy Act. Clearly establishing a senior official as a focal point for departmental privacy functions aligns with direction provided by law and OMB and would help ensure that the agency provides consistent privacy protections.

The Senior Agency Official for Privacy at the Department of Defense stated that, while privacy responsibilities are divided among the Defense Privacy Office, the CIO, and agency components, the current privacy management structure at Defense has proven to be successful over time. We did not assess the effectiveness of the privacy management structures we reviewed. However, establishing an agency official that serves as a central focal point for departmental privacy functions aligns with direction provided by law and OMB and would help ensure that the agency provides consistent privacy protections.

The Acting Chief Privacy and Civil Liberties Officer at Justice disagreed with our assessment that the department's SAOP did not have oversight of redress procedures. He stated that the Chief Privacy and Civil Liberties Officer has statutory authority under the Violence Against Women and Department of Justice Reauthorization Act to assume primary responsibility for privacy policy and to ensure appropriate notifications regarding the department's privacy policies and privacy-related inquiry and complaint procedures. We agree that the Chief Privacy and Civil Liberties officer has the statutory authority and responsibility for the oversight of privacy functions at Justice, including redress. However, our analysis of agency policies and procedures showed that the Chief Privacy and Civil Liberties Officer did not have an established role in oversight of redress procedures. Clearly defining the role of the Chief Privacy and Civil Liberties Officer in the departmental redress procedures would help ensure that the SAOP has oversight of this key privacy function. In its comments, the department noted that the Office of Privacy and Civil Liberties was undertaking a review of its orders and guidance to clarify and, as appropriate, strengthen existing authorities to ensure that the

department implements thoroughly the Chief Privacy and Civil Liberties Officer authorities.

The Chief Information Officer at Labor disagreed with our assessment that the SAOP did not have full oversight of all key privacy functions. He stated that Privacy Act compliance, redress, and training were addressed jointly by his office and the Office of the Solicitor. However, our review of Labor's policies and procedures relating to privacy management showed that a joint oversight management structure had not been established. Rather, we found that while the CIO was responsible for three key privacy functions, the Office of the Solicitor was responsible for the remaining three functions. Clearly defining the role of the SAOP in Privacy Act compliance, redress, and training would help ensure that the SAOP has oversight of all key privacy functions.

The Assistant Secretary for Management at Treasury agreed that the SAOP should have overall responsibility for privacy protection and compliance with statutory requirements and that agencies generally would likely benefit from having SAOPs that serve as central focal points for privacy matters and have oversight of all key functions. The Assistant Secretary noted that as of March 2008, the department had implemented a new privacy management structure to emphasize the importance of protecting privacy at its highest levels. However, Treasury disagreed with a statement in our draft report that it had realigned its organization in order to ensure that the SAOP had oversight of privacy functions. We recognize that privacy functions, with the exception of redress, were under the oversight of the SAOP prior to the reorganization and accordingly have deleted this statement from the final report. Treasury also disagreed that its SAOP did not have full oversight of agency redress processes, stating that the department has longstanding regulations that provide departmentwide and bureau-specific policies and procedures relating to redress. While we agree that such redress policies are in place, they do not establish a role for the SAOP. Clearly defining the role of the SAOP in the departmental redress procedures would help ensure that the SAOP has oversight of this key privacy function. Lastly, Treasury stated it submits quarterly reports to Congress on privacy complaint and redress activities. We agree that reporting is an important privacy function; however, it is separate from redress and does not constitute oversight of Treasury redress activities.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Attorney General; the Secretaries of Commerce, Defense, Health and Human Services, Homeland Security, State, Treasury, Labor, Transportation, and Veterans Affairs; the Commissioner of the Social Security Administration; and the Administrator of the U.S. Agency for International Development as well as other interested congressional committees. Copies will be made available at no charge on our Web site, www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6240 or send e-mail to koontzl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Sincerely,

Linda D. Koontz
Director, Information Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe laws and guidance that set requirements for senior privacy officials within federal agencies, and (2) describe the organizational structures used by agencies to address privacy requirements and assess whether senior officials have oversight over key functions. We did not evaluate agency compliance with these laws and guidance.

To address our first objective, we reviewed and analyzed relevant laws and guidance to determine privacy responsibilities for privacy officials at agencies. We reviewed relevant laws, including the Implementing Recommendations of the 9/11 Commission Act of 2007, the Homeland Security Act of 2002, and others (see app. II for a full listing), which designate senior privacy officials and assign them privacy responsibilities. We also analyzed the Paperwork Reduction Act, which has long-standing privacy requirements assigned to agency chief information officers (CIO), and the Office of Management and Budget (OMB) guidance relating to the designation of senior agency officials with privacy responsibilities, such as Memorandum M-05-08. We also analyzed the specific privacy responsibilities identified in these laws and guidance and categorized the key privacy functions they represented.

To address our second objective, we identified 12 agencies (Departments of Commerce, Defense, Health and Human Services, Homeland Security, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs; the Social Security Administration, and the U.S. Agency for International Development) that either have a statutorily designated privacy officer, have a central mission for which privacy protection is a critical component, or have implemented a unique organizational privacy structure. We analyzed policies and procedures at these agencies, and interviewed senior agency privacy officials to identify the privacy management structures used at each of these agencies and the roles and responsibilities of senior privacy officials. We also compared the varying management structures at these agencies to identify the differences and similarities across agencies in their implementation of these structures. Further, we analyzed agency management structures to determine whether senior privacy officials at each of these agencies had full oversight over all key functions.

We conducted our work from September 2007 to May 2008, in Washington, D.C., in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MAY 12 2008

Ms. Linda Koontz
Director, Information Management Issues
Government Accountability Office
441 G. Street, N.W.
Washington, D.C. 20548

Dear Ms. Koontz:

Thank you for the opportunity to review the draft of GAO 310794 – *Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions.*

The report is useful in illustrating the diverse ways agencies carry out their privacy responsibilities and the fragmentation that exists as a result of recent laws and guidance that have significantly changed requirements for privacy oversight and management. The laws and guidance vary in scope and specificity, but as the report indicates, require the designation of a Senior Agency Official for Privacy with overall responsibility for privacy protection and compliance with statutory requirements.

However, the report appears to indicate that existing laws and guidance require that agencies organize their internal privacy functions, including the administration of the Privacy Act, so that, for example, at the Department of Commerce they would be consolidated under the direct supervision of, and report to, the Commerce Chief Information Officer, who is the designated Senior Agency Official for Privacy and the Chief Privacy Officer. It is our view that applicable law does not require that administration of the Privacy Act be consolidated with other privacy functions under the Office of the Chief Information Officer. In fact, at Commerce, the Privacy Act is administered under the Chief Financial Officer and Assistant Secretary for Administration, who coordinates with the Office of the Chief Information Officer on Privacy Act issues. The Chief Privacy Officer provides oversight and guidance on privacy issues, but does not handle Privacy Act requests or appeals.

Indeed, agencies are accorded some flexibility precisely to provide the opportunity to organize their privacy functions in the way that works best for each of them. Since its enactment in 1974, administration of the Privacy Act has at Commerce been the responsibility of the Chief Financial Officer and Assistant Secretary for Administration. The Commerce Privacy Act program is well regarded, and cooperates fully with the Chief Privacy Officer with regard to all privacy functions within the Office of the Chief Information Officer.

We see no reason to upset this well-coordinated well-functioning institutional arrangement absent specific and explicit requirements to do so. We would expect that other agencies would have similar interests in maintaining existing organizational arrangements that they have found effective in providing privacy oversight, coordination, and protection.

Sincerely,

Suzanne Hilding
Chief Information Officer

Appendix III: Comments From the Department of Defense

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION &
MANAGEMENT

MAY 1 3 2008

MEMORANDUM FOR UNITED STATES GOVERNMENT ACCOUNTIBILITY OFFICE

SUBJECT: Conclusions and recommendations from Draft GAO Report titled:
PRIVACY: Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions (GAO-08-603)

The DoD appreciates the opportunity to comment on the subject report. The report concluded that "not all agencies gave their Senior Agency Official for Privacy (SAOP) responsibility for all key privacy functions. The single recommendation made was "In order to ensure that their SAOPs function effectively as central focal points for privacy management, we recommend that the Attorney General and the Secretaries of Commerce, Defense, Health and Human Services, Labor, and Treasury take steps to ensure that their SAOPs have oversight over all key privacy functions.

The Director, Administration and Management for the DoD is assigned as the SAOP. In this role, he has direct oversight of the core privacy functions and executes these through the Defense Privacy Office. This office administers the Privacy Act of 1974 and the other privacy functions required by various laws. The area of redress of complaints and inquiries has been further delegated to the DoD Components who are the liaison organizations between DoD and the various systems owners located within the components. The process to address these issues has been found to be most effective when resolved at this level in the organization.

The DoD CIO serves as the DoD principal point of contact for Information Technology (IT) matters, oversees the PIAs and the protection of information in IT. The Office of the DoD CIO works closely with the Defense Privacy Office on all matters involving IT privacy policy and implementation. Per our DoD PIA guidance, the DoD SAOP serves as the DoD principal point of contact for the privacy policies and provides assistance on privacy matters impacting PIAs. The review of completed PIAs and annual reporting of the completion of these assessments is conducted with the Defense Privacy Office and other DoD Components as required. This arrangement has proven to be successful over time.

The DoD CIO concurs in this response. Questions regarding this response should be directed to Samuel Jenkins, Director, Defense Privacy Office at (703) 607-2943 or via email at DPO.Correspondence@osd.mil.

Michael B. Donley
Senior Agency Official for Privacy

Appendix IV: Comments From the Department of Justice

U.S. Department of Justice

Office of the Deputy Attorney General

Chief Privacy and Civil Liberties Officer

Washington, D.C. 20530

May 12, 2008

Linda D. Koontz
Director
Information Management
Government Accountability Office
441 G. Street, NW
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled, "Privacy: Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions" (GAO-08-603). The Department of Justice is pleased that this report acknowledges that the Department of Justice has taken important and significant steps in ensuring the effectiveness of its privacy official and embedding the protection of privacy and civil liberties into the fabric of the Department.

We would like to address GAO's statement that the Department of Justice's Chief Privacy and Civil Liberties Officer (CPCLO), the Department's Senior Agency Official for Privacy (SAOP), does not have oversight concerning the redress mechanisms associated with the Department's handling of personally identifiable information (PII).

We disagree that this oversight function does not already lie with the CPCLO. At the core of the statutorily mandated activities of the CPCLO is section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, January 5, 2006. Specifically, subsection (a) provides that "[t]he Attorney General shall designate a senior official in the Department of Justice to assume primary responsibility for privacy policy." Subsequently, on March 10, 2006, Deputy Attorney General Paul McNulty issued a memorandum, which designated this senior official, stating that "[a]s the CPCLO, the official will oversee and administer the Department's privacy functions, in accordance with [section 1174]."

As such, the CPCLO does already have full responsibility for the oversight and management of all the privacy functions associated with the Department and its constituent components. Although it is true that the various components deal with day-to-day aspects of the operations concerning privacy functions, the CPCLO administers such functions through the promulgation of appropriate policies, the leadership of Departmental privacy officers, and the provision of specific guidance as required.

Further, section 1174(b) notes specific responsibilities of the CPCLO, including under subsection (5), "appropriate notifications regarding the Department's privacy policies and privacy-related inquiry and complaint procedures," which deal with the redress processes at the

Department. In addition, section 1162 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, December 17, 2005, was amended by section 805 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, August 3, 2007, to provide, in part, that agency privacy officials "ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and *redress* complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties." [Emphasis added] As such, even if the general requirement for the CPCLO to oversee all the privacy functions of the Department were not enough authority to exercise leadership over the Department's redress processes, these additional two statutory authorities create a specific mandate for the CPCLO to fulfill.

Nonetheless, the Department, through its Office of Privacy and Civil Liberties is undertaking a review of the existing orders and guidance issued by the Department to clarify and, as appropriate, strengthen these existing authorities. The goal of this endeavor is to ensure that the Department implements thoroughly the CPCLO's authorities and to increase awareness of these authorities by all parts of the Department.

Again, we appreciate the opportunity to comment on GAO's draft report, and we look forward to additional collaboration to ensure full application of privacy protective authorities government wide. If you have any questions regarding our comments, please contact Richard P. Theis, Department of Justice Audit Liaison, Audit Liaison Group at (202) 514-0469.

Respectfully submitted,

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer

Appendix V: Comments from the Department of Labor

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

MAY 12 2008

Linda D. Koontz
Director, Information Management Issues
Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Koontz:

This letter responds to draft report GAO 08-603, *Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions*, dated May 2008. We take seriously our responsibility to ensure the protection of our computer systems, web-based resources and collection points for Personally Identifiable Information (PII) and appreciate the opportunity to comment on the draft report.

Overall, the draft report provides a fair depiction of the Department of Labor's (DOL) management and operating environment for the protection of PII. However, I ask that the representation of how responsibilities for the key privacy functions are overseen at DOL be revised. As the Chief Information Officer (CIO) and Senior Agency Official for Privacy (SAOP), I have responsibility for *all* key privacy functions. In addition, three of the key privacy functions—namely, Privacy Act compliance, Redress, and Training—are jointly addressed by my office and the Department's Office of the Solicitor. This process has worked well for the Department in meeting our privacy protection related responsibilities.

With this in mind, to accurately reflect DOL's management structure for meeting its privacy protection responsibilities, the draft report should be revised in two areas:

- On page 20, Figure 2 should show for the Department of Labor that the SAOP is the CIO who has primary responsibility for all key privacy functions, including joint responsibility with the Office of the Solicitor for the three privacy functions of Privacy Act compliance, Redress, and Training. This management structure appears very similar to that portrayed in Figure 2 for the Department of Transportation.
- Correspondingly, the draft report Recommendation on page 24 should be amended to remove reference to the Department of Labor in addition to other conforming revisions throughout the draft report.

Thank you again for the opportunity to comment on the draft report. If there are questions or further discussion about our comments is needed, please have your staff contact Ms. Tonya Manning, Chief Information Security Officer, at Manning.Tonya@dol.gov or 202-693-4431.

Sincerely,

Patrick Pizzella
Assistant Secretary for Administration and Management,
Chief Information Officer

Appendix VI: Comments from the Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

MAY 1 5 2008

Mr. Idris Adjerid
Analyst-in-Charge
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Adjerid:

Thank you for the opportunity to review and comment on your draft report entitled "PRIVACY: Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions", GAO-08-603. The Treasury Department concurs with your conclusions that the Senior Agency Official for Privacy (SAOP) should have overall responsibility for privacy protection and compliance with statutory requirements and that agencies generally would likely benefit from having SAOPs that serve as central focal points for privacy matters and have oversight of all key functions, because such focal points can help ensure that agency activities provide consistent privacy protections.

The policy of the Department of the Treasury is to protect the privacy of individuals by ensuring that due consideration and regard for information privacy is addressed in the execution of Departmental programs and policies. To emphasize the importance of protecting privacy at the highest levels of the Department, and to assign accountability, the Department has designated the Assistant Secretary for Management and Chief Financial Officer (ASM/CFO) as the SAOP pursuant to Office of Management and Budget Memorandum OMB M-05-08. The ASM/CFO has also been designated as the Chief Privacy Officer, pursuant to Section 522 of Division H of the Consolidated Appropriations Act of 2005, and the Chief Privacy and Civil Liberties Officer, pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

The ASM/CFO has historically had overall responsibility for key privacy functions. Nonetheless, in order to strengthen oversight of this important area, the Department realigned components of the Office of the ASM/CFO on March 24, 2008, to create a new Office of the Deputy Assistant Secretary for Privacy and Treasury Records. The realignment combined the Privacy Act and E-Government Act privacy functions and programs into one office and elevated the importance of the privacy office by creating a new Deputy Assistant Secretary for Privacy and Treasury Records, who is a direct report to the ASM/CFO. The Department continues to review a wide variety of activities and procedures within the Department to find opportunities to enhance protections of the privacy of individuals.

In that light, we respectfully request that your statement on page 22, that Treasury was reorganizing in order to ensure that the SAOP had overall responsibility for key privacy functions, be amended to reflect that the Treasury SAOP has historically had overall responsibility for key privacy functions, and has also now realigned its privacy functions from two offices into one office and has elevated the position of that office within the organization. In conjunction, we also request that your statement on page 23, that Treasury is currently considering consolidating privacy functions under a central office reporting directly to the SAOP, be amended to reflect that Treasury has, as of March 2008, consolidated its privacy functions from two Management divisions into one Management office reporting directly to the SAOP.

On page 15, the draft report defines redress in the privacy context as an agency's complaint-resolution process that allows individuals access to their records and the ability to correct inaccurate information, pursuant to the Privacy Act of 1974. On pages 6 and 15, the draft report presents federal agency redress responsibilities as ensuring that redress procedures are in place; that is, ensuring adequate procedures for investigating and addressing privacy complaints by individuals. Regarding the chart on page 20 and your statement on page 21, that the SAOP does not have oversight over the Treasury privacy redress function, we point out that Treasury has long-standing regulations at 31 C.F.R. §§ 1.26 and 1.27, that provide Treasury-wide procedures for redress in the privacy context. In addition, each Treasury bureau has specific, additional procedures published in Appendix A to Subpart C of 31 C.F.R. Part 1, tailored to the mission and functions of the particular bureau. These bureau-specific procedures have been fully approved and authorized by the Department. Moreover, Treasury has developed and implemented binding Department-wide policy and procedures in Treasury Directive 25-04 and The Privacy Handbook, TD Publication 25-04. In fact, Treasury Directive 25-04 stipulates that the ASM/CFO is responsible for ensuring Treasury's compliance with the Privacy Act of 1974.

Finally, the SAOP submits to Congress quarterly reports of Department-wide privacy complaint and redress activities, pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. In addition to these procedures for providing redress, we continue to look for improvements that can be made to the Treasury redress process. In light of existing redress procedures as spelled out above, we respectfully request that the chart on page 20 and the statement on page 21of the draft report be amended to reflect that the Treasury SAOP does have oversight responsibilities over Treasury redress functions in the privacy context.

Again, we appreciate the opportunity to comment on GAO's draft report. If you have any questions regarding our comments, please contact me, or Elizabeth Cuffe of my staff, at 202-622-1682 or by email at Elizabeth.Cuffe@do.treas.gov.

Sincerely,

Peter B. McCarthy
Assistant Secretary for Management
and Chief Financial Officer

Appendix VII: Recent Laws Establishing Privacy Protection Responsibilities at Federal Agencies

The following are recent laws and their major provisions regarding privacy protection responsibilities at federal agencies.

Homeland Security Act of 2002

Section 222 of the Homeland Security Act of 2002, [1] as amended, instructed the secretary of DHS to appoint a senior official with primary responsibility for privacy policy, including the following:

- ensuring that technologies sustain, and do not erode, privacy protections;
- ensuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the act;
- evaluating legislative and regulatory proposals and conducting privacy impact assessments of proposed rules;
- coordinating functions with the Officer for Civil Rights and Civil Liberties;
- preparing an annual report to Congress (without prior comment or amendment by agency heads or OMB); and
- having authority to investigate and having access to privacy-related records, including through subpoena in certain circumstances.

Intelligence Reform and Terrorism Prevention Act of 2004

Section 1011 of this act required the Director of National Intelligence to appoint a Civil Liberties Protection Officer and gave this officer the following functions:[2]

- ensuring that the protection of civil liberties and privacy is appropriately incorporated into the policies and procedures of the Office of the Director of National Intelligence and the elements of the intelligence community within the National Intelligence Program;

[1]Pub. L. No. 107-296, November 25, 2002, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, Sec. 8305, and the Implementing Recommendations of the 9/11 Commission Act of 2007, Sec. 802.

[2]Pub. L. No. 108-458, December 17, 2004.

- overseeing compliance by the Office of the Director of National Intelligence with all laws, regulations, and guidelines relating to civil liberties and privacy;
- reviewing complaints about abuses of civil liberties and privacy in Office of the Director of National Intelligence programs and operations;
- ensuring that technologies sustain, and do not erode, privacy protections;
- ensuring that personal information contained in a system of records subject to the Privacy Act is handled in full compliance with fair information practices as set out in that act;
- conducting privacy impact assessments when appropriate or as required by law; and
- performing such other duties as may be prescribed by the Director of National Intelligence or specified by law.

Violence Against Women and Department of Justice Reauthorization Act of 2005

Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005[3] instructed the Attorney General to designate a senior official to assume primary responsibility for privacy policy, which included responsibility for advising the Attorney General in the following areas:

- appropriate privacy protections for the department's existing or proposed information technology and systems;
- privacy implications of legislative and regulatory proposals;
- implementation of policies and procedures, including training and auditing, to ensure compliance with privacy-related laws and policies;
- that adequate resources and staff are devoted to meeting the department's privacy-related functions and obligations;
- appropriate notifications regarding privacy policies and inquiry and complaint procedures; and

[3]Pub. L. No. 109-162, January 5, 2005

- privacy-related reports from the department to Congress and the President, including an annual report to Congress on activities affecting privacy.

Transportation, Treasury, Independent Agencies and General Government Appropriations Act of 2005

Section 522 of this act[4] directed each agency with appropriations provided by the act to designate a chief privacy officer with primary responsibility for privacy and data protection policy, including

- ensuring that technology sustains, and does not erode, privacy and that technology used to collect or process personal information allows for continuous auditing of compliance with stated privacy policies and practices;
- ensuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act;
- evaluating legislative and regulatory proposals and conducting privacy impact assessments of proposed rules;
- preparing an annual report to Congress on activities affecting privacy;
- ensuring the protection of personal information and information systems from unauthorized access, use, disclosure, or destruction,
- providing employees with privacy training; and
- ensuring compliance with privacy and data protection policies.

Implementing Recommendations of the 9/11 Commission Act of 2007

This law[5] amended the National Intelligence Reform Act of 2004 to require the heads of covered agencies to designate no less than one senior officer to serve as a privacy and civil liberties officer. This act applies to the Departments of Defense, Homeland Security, Justice, Treasury, Health and Human Services, and State, as well as the Office of the Director of National Intelligence, and the Central Intelligence Agency. The act requires the senior privacy official to perform the following functions:

[4]Div H, Pub. L. No. 108-447, December 8, 2004.

[5]Pub. L. No. 110-53 August 3, 2007.

- assisting the agency head in considering privacy and civil liberties issues with regard to anti-terrorism efforts;
- investigating and reviewing agency actions to ensure adequate consideration of privacy and civil liberties;
- ensuring that the agency has adequate redress procedures,
- considering privacy and civil liberties when deciding to retain or enhance a governmental power;
- coordinating activities, when relevant, with the agency Inspector General; and
- preparing periodic reports, not less than quarterly, to the agency head, Congress, and the Privacy and Civil Liberties Oversight Board.[6]

Agencies covered under this act are also required to establish a direct reporting relationship between the senior privacy official and the agency head.

[6]This board was created by the Intelligence Reform and Terrorism Prevention Act of 2004 to review executive branch anti-terrorism activities and to ensure that privacy and civil liberties are adequately protected.

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

Linda D. Koontz, (202) 512-6240, koontzl@gao.gov

Staff Acknowledgments

Major contributors to this report were John de Ferrari, Assistant Director; Idris Adjerid; Shaun Byrnes; Matt Grote; David Plocher; Jamie Pressman; and Amos Tevelow.

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548