United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2007

DHS PRIVACY OFFICE

Progress Made but Challenges Remain in Notifying and Reporting to the Public

GAO-07-522

April 2007

DHS PRIVACY OFFICE

Progress Made but Challenges Remain in Notifying and Reporting to the Public

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-522, a report to congressional requesters

Why GAO Did This Study

The Department of Homeland Security (DHS) Privacy Office was established with the appointment of the first Chief Privacy Officer in April 2003, as required by the Homeland Security Act of 2002. The Privacy Office's major responsibilities include: (1) reviewing and approving privacy impact assessments (PIA)—analyses of how personal information is managed in a federal system, (2) integrating privacy considerations into DHS decision making, (3) ensuring compliance with the Privacy Act of 1974, and (4) preparing and issuing annual reports and reports on key privacy concerns.

GAO's objective was to examine progress made by the Privacy Office in carrying out its statutory responsibilities. GAO did this by comparing statutory requirements with Privacy Office processes, documents, and activities.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security take several actions including appointing privacy officers in key DHS components, implementing a process for reviewing Privacy Act notices, and establishing a schedule for timely issuance of Privacy Office reports.

DHS generally agreed with the content of this report and its recommendations and described actions initiated to address GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-522.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz, 202-512-6240 or koontzl@gao.gov.

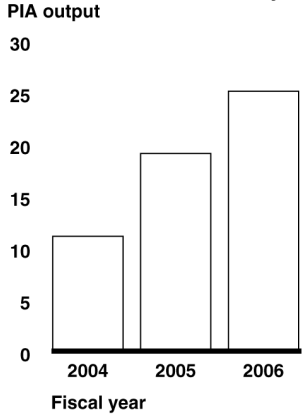
What GAO Found

The DHS Privacy Office has made significant progress in carrying out its statutory responsibilities under the Homeland Security Act and its related role in ensuring compliance with the Privacy Act of 1974 and E-Government Act of 2002, but more work remains to be accomplished. Specifically, the Privacy Office has made significant progress by establishing a compliance framework for conducting PIAs, which are required by the E-Gov Act. The framework includes formal written guidance, training sessions, and a process for identifying affected systems. The framework has contributed to an increase in the quality and number of PIAs issued (see fig.) as well as the identification of many more affected systems. The resultant workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain DHS components could help speed processing of PIAs, but DHS has not yet taken action to make these designations.

The Privacy Office has also taken actions to integrate privacy considerations into the DHS decision-making process by establishing an advisory committee, holding public workshops, and participating in policy development. However, limited progress has been made in updating public notices required by the Privacy Act for systems of records that were in existence prior to the creation of DHS. These notices should identify, among other things, the type of data collected, the types of individuals about whom information is collected, and the intended uses of the data. Until the notices are brought up-to-date, the department cannot assure the public that the notices reflect current uses and protections of personal information.

Further, the Privacy Office has generally not been timely in issuing public reports. For example, a report on the Multi-state Anti-Terrorism Information Exchange program—a pilot project for law enforcement sharing of public records data—was not issued until long after the program had been terminated. Late issuance of reports has a number of negative consequences, including a potential reduction in the reports' value and erosion of the office's credibility.

Number of PIAs for DHS Systems Published by Fiscal Year



Source: GAO analysis of published DHS PIAs.

Contents

Abbreviations

CBP	Customs and Border Protection
DHS	Department of Homeland Security
E-Gov Act	E-Government Act
FOIA	Freedom of Information Act
MATRIX	Multi-state Anti-Terrorism Information Exchange
OCIO	Office of the Chief Information Officer
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
PIA	privacy impact assessment
PTA	privacy threshold analysis
TSA	Transportation Security Administration
RFID	radio frequency identification
US-VISIT	U.S. Visitor and Immigrant Status Indicator

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

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 27, 2007

Congressional Requesters

As you know, the Homeland Security Act of 2002 created the first statutorily required senior privacy official at any federal agency. This law mandated the appointment of a senior official at the Department of Homeland Security (DHS) to assume primary responsibility for privacy policy, including, among other things, assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information.[1] The DHS Privacy Office was formally established with the appointment of the first DHS Chief Privacy Officer on April 16, 2003.

The Privacy Office is responsible for ensuring that DHS is in compliance with federal laws that govern the use of personal information by the federal government. Among these laws are the Homeland Security Act of 2002 (as amended by the Intelligence Reform and Terrorism Prevention Act of 2004), the Privacy Act of 1974, and the E-Government Act of 2002. [2] 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 uses of the data, and procedures that individuals can use to review and correct personal information. The E-Government Act (E-Gov Act) requires agencies to conduct privacy impact assessments (PIA) of privacy risks associated with information technology used to process personal information.[3] In addition, the Privacy Office is required by the Homeland Security Act to report annually on its activities, and it has been directed by Congress to prepare reports on specific topics. The Privacy Office's major responsibilities can be summarized into four broad categories: (1) reviewing and approving PIAs, (2) integrating privacy considerations

[1]Homeland Security Act of 2002, Sec. 222, Pub. L. 107-296 (Nov. 25, 2002).

[2]Section 222 of the Homeland Security Act, as amended by section 8305 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec. 17, 2004), 6 U.S.C. § 142; Privacy Act of 1974, 5 U.S.C. § 552a; section 208 of the E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

[3]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.

into DHS decision making, (3) reviewing and approving public notices required by the Privacy Act, and (4) preparing and issuing reports.

You asked us to examine progress made by the Privacy Office in implementing its statutory requirements. Specifically, as agreed with your staff, our objective was to assess the progress of the DHS Privacy Office in carrying out its responsibilities under federal privacy laws, including the Homeland Security Act and the E-Gov Act.

To address our objective, we analyzed the Homeland Security Act and other relevant laws and regulations to identify DHS Privacy Office responsibilities. We analyzed Privacy Office policies, guidance, and reports, and interviewed Privacy Office officials to assess plans, priorities, and processes for implementing statutory requirements using available resources. We assessed progress made by the Privacy Office by comparing this information against its statutory responsibilities. We evaluated Privacy Office policies, guidance, and processes to ensure compliance with the E-Gov Act of 2002 and the Privacy Act of 1974, including PIA and system-of-records notice processes, and assessed the progress made by the office in implementing these processes. We also interviewed former chief privacy officers, privacy advocacy groups, cognizant component-level officials, and members of the DHS Data Privacy and Integrity Advisory Committee. Our work was performed in accordance with generally accepted government auditing standards. Our objective, scope, and methodology are discussed in more detail in appendix I.

Results in Brief

The DHS Privacy Office has 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 more work remains to be accomplished. Specifically, the Privacy Office has established processes for ensuring departmental compliance with the PIA requirement in the E-Gov Act. It has done this by developing a compliance framework that includes formal written guidance, a template for conducting assessments, training sessions, a process for identifying systems that require assessments, and a process for reviewing and approving assessments. Instituting this framework has led to increased attention to privacy requirements on the part of departmental components, contributing to an increase in the quality and number of PIAs issued. It has also proved beneficial in identifying systems that require an assessment, from 46 identified in fiscal year 2005 to a projected 188 in fiscal year 2007. However, the resulting increase in the workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain key

DHS components could help speed processing of PIAs, but DHS has not yet done this.

The Privacy Office has taken actions to integrate privacy considerations into the DHS decision-making process through a variety of actions, including establishing a federal advisory committee, raising awareness of privacy issues through a series of public workshops, and participating in policy development for several major departmental initiatives. These actions serve, in part, to address the mandate to assure technologies sustain and do not erode privacy protections. The Privacy Office's participation in policy decisions provides an opportunity for privacy concerns to be raised explicitly and considered in the development of DHS policies. In addition, the office has taken steps to address its mandates to evaluate regulatory and legislative proposals involving personal information and to coordinate with the DHS Officer for Civil Rights and Civil Liberties.

While substantial progress has been made in these areas, limited progress has been made in other important aspects of privacy protection. For example, while the Privacy Office has reviewed, approved, and issued 56 new and revised Privacy Act public notices since its establishment, little progress has been made in updating notices for "legacy" systems of records—older systems of records that were originally developed by other agencies prior to the creation of DHS. According to Privacy Office officials, they have focused their attention on reviewing and approving PIAs and developing notices for new systems and have given less priority to revising notices for legacy systems. However, because many of these notices are not up-to-date, the department cannot be assured that the privacy implications of its many systems that process and maintain personal information have been fully and accurately disclosed to the public.

Further, the Privacy Office has generally not been timely in issuing public reports, potentially limiting their value and impact. The Homeland Security Act requires that the Privacy Officer report annually to Congress on its activities, including complaints of privacy violations. However, the office has issued only two annual reports within the 3-year period since it was established in April 2003, and one of these did not include complaints of privacy violations as required. In addition, other reports to Congress on several specific topics have been late. The office also initiated its own investigations of specific programs and produced reports on these reviews, but several of them were not publicly released until long after concerns had been addressed. For example, a report on the Multi-state

Anti-Terrorism Information Exchange program—a pilot project for law enforcement sharing of public records data—was not issued until long after the program had been terminated. Late issuance of reports has a number of negative consequences beyond failure to comply with mandated deadlines, including a potential reduction in the reports' value and erosion of the office's credibility.

We are making recommendations to the Secretary of Homeland Security to designate component-level privacy officers at key components, ensure that Privacy Act notices reflect current DHS activities, and help the Privacy Office meet its obligations and issue reports in a timely manner.

In its written comments on a draft of this report, DHS generally agreed with our recommendations and described actions initiated to address them.

Background

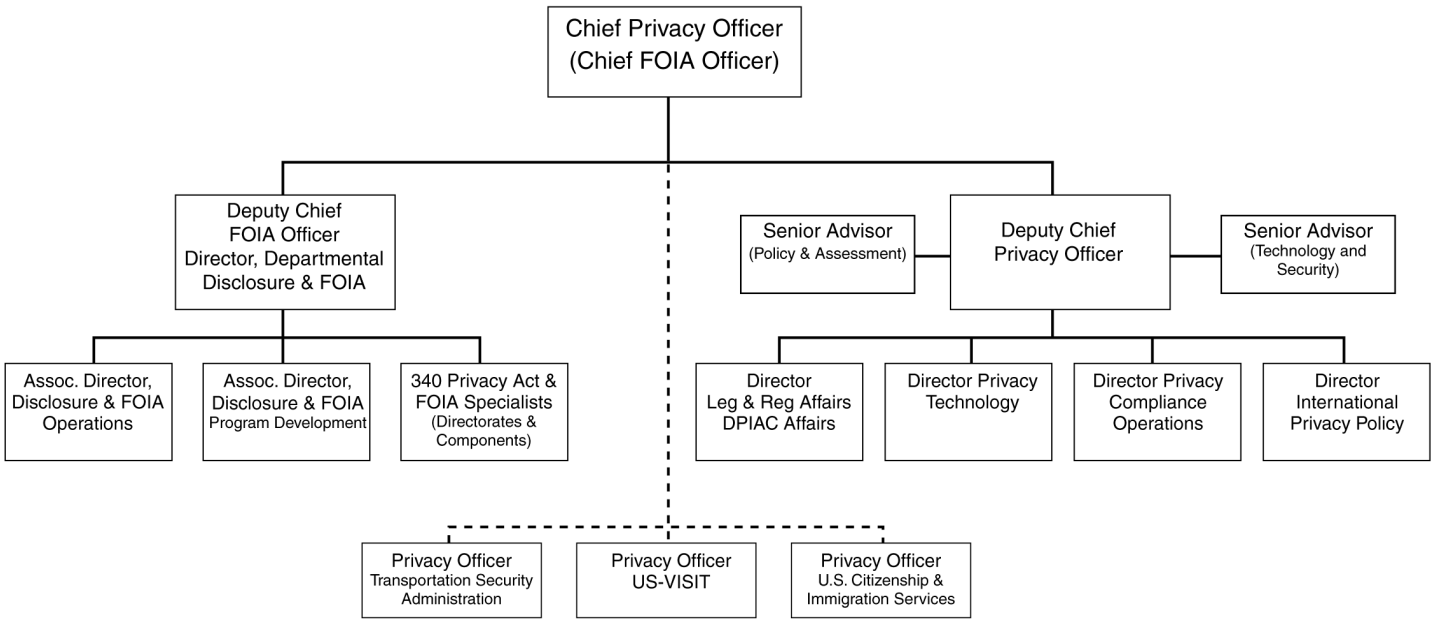
The DHS Privacy Office was established with the appointment of the first Chief Privacy Officer in April 2003. The Chief Privacy Officer is appointed by the Secretary and reports directly to him. Under departmental guidance, the Chief Privacy Officer is to work closely with other departmental components, such as the General Counsel's Office and the Policy Office, to address privacy issues. The Chief Privacy Officer also serves as the designated senior agency official for privacy, as has been required by the Office of Management and Budget (OMB) of all major departments and agencies since 2005.[4]

The positioning of the Privacy Office within DHS differs from the approach used for privacy offices in other countries, such as Canada and the European Union, where privacy offices are independent entities with investigatory powers. Canada's Privacy Commissioner, for example, reports to the Canadian House of Commons and Senate and has the power to summon witnesses and subpoena documents. In contrast, the DHS privacy officer position was established by the Homeland Security Act as an internal component of DHS. As a part of the DHS organizational structure, the Chief Privacy Officer has the ability to serve as a consultant on privacy issues to other departmental entities that may not have adequate expertise on privacy issues.

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

The office is divided into two major functional groups addressing Freedom of Information Act (FOIA)[5] and privacy responsibilities, respectively. Within each functional group, major responsibilities are divided among senior staff assigned to oversee key areas, including international privacy policy, departmental disclosure and FOIA, privacy technology, and privacy compliance operations. There are also component-level and program-level privacy officers at the Transportation Security Administration (TSA), U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, and U.S. Citizenship and Immigration Services. Figure 1 details the structure of the DHS Privacy Office.

Figure 1: DHS Privacy Office Organizational Structure



Source: GAO analysis of DHS data.

[5]Our review did not include an assessment of the Privacy Office's FOIA responsibilities.

When the Privacy Office was initially established, it had 5 full-time employees, including the Chief Privacy Officer. Since then, the staff has expanded to 16 full-time employees. The Privacy Office has also hired private contractors to assist in meeting its obligations. As of February 2007, the Privacy Office had 9 full-time and 3 half-time contractor staff in addition to its full-time employees. The first Chief Privacy Officer served from April 2003 to September 2005, followed by an Acting Chief Privacy Officer who served through July 2006. In July 2006, the Secretary appointed a second permanent chief privacy officer.

In 2004, the Chief Privacy Officer established the DHS Data Privacy and Integrity Advisory Committee, which is to advise the Secretary and the Chief Privacy Officer on "programmatic, policy, operational, administrative, and technological issues within DHS" that affect individual privacy, data integrity, and data interoperability. The Advisory Committee is composed of privacy professionals from the private sector and academia and is organized into three subcommittees; Data Integrity and Information Protection, Privacy Architecture, and Data Acquisition and Use. To date, the Advisory Committee has issued reports on several privacy issues, such as use of commercial data and radio frequency identification (RFID)[6] technology, and has made related policy recommendations to the department. The Advisory Committee's charter requires that the committee meet at least once a year; however, thus far it has met quarterly. The Advisory Committee meetings, which are open to the public, are used to discuss progress on planned reports, to identify new issues, to receive briefings from DHS officials, and to hold panel discussions on privacy issues.

Privacy Office Responsibilities

The Privacy Office is responsible for ensuring that DHS is in compliance with federal laws that govern the use of personal information by the federal government. Among these laws are the Homeland Security Act of 2002 (as amended by the Intelligence Reform and Terrorism Prevention Act of 2004), the Privacy Act of 1974, and the E-Gov Act of 2002. Based on these laws, the Privacy Office's major responsibilities can be summarized into four broad categories: (1) reviewing and approving PIAs, (2) integrating privacy considerations into DHS decision making,

[6]RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. RFID technology provides identification and tracking capabilities by using wireless communication to transmit data.

(3) reviewing and approving public notices required by the Privacy Act, and (4) preparing and issuing reports.

Reviewing and approving PIAs

Section 208 of the E-Gov Act is designed to enhance protection of personally identifiable information in government information systems and information collections by requiring that agencies conduct PIAs. According to OMB guidance,[7] a PIA is an analysis of how information is handled: (1) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating personally identifiable information in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential risks to privacy.

Agencies must conduct PIAs before they (1) develop or procure information technology that collects, maintains, or disseminates personally identifiable information or (2) initiate any new data collections of 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,[8] they provide explanations to the public about such things as what information 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. Further, a PIA can serve as a tool to guide system development decisions that have a privacy impact.

The Privacy Office is responsible for ensuring departmental compliance with the privacy provisions of the E-Gov Act. Specifically, the chief privacy officer must ensure compliance with the E-Government Act requirement that agencies perform PIAs. In addition, the Homeland Security Act requires the chief privacy officer to conduct a PIA for proposed rules of the department on the privacy of personal information. The Privacy Office's involvement in the PIA process also serves to address the

[7]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).

[8]Section 208(b)(1)(B)(iii) of the E-Gov Act requires agencies, if practicable, to make PIAs publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. 107-347 (Dec. 17, 2002).

Homeland Security Act requirement that the chief privacy officer assure that technology sustains and does not erode privacy protections.

Integrating privacy considerations into the DHS decision-making process

Several of the Privacy Office's statutory responsibilities involve ensuring that the major decisions and operations of the department do not have an adverse impact on privacy. Specifically, the Homeland Security Act requires that the Privacy Office assure that the use of technologies by the department sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. The act further requires that the Privacy Office evaluate legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government. It also requires the office to coordinate with the DHS Officer for Civil Rights and Civil Liberties on those issues.

Reviewing and approving public notices required by the Privacy Act

The Privacy Office is required by the Homeland Security Act to assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974. The Privacy Act places limitations on agencies' collection, disclosure, and use of personally identifiable information that is maintained in their systems of records. The act defines a record as any item, collection, or grouping of information about an individual that is maintained by an agency and contains that individual's name or other personal identifier, such as a Social Security number. It 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 agencies to notify the public, via a notice in the *Federal Register*, when they create or modify a system-of-records. This notice is known as a system-of-records notice and must include information such as the type of information collected, the types of individuals about whom information is collected, the intended "routine" uses of the information, and procedures that individuals can use to review and correct their personal information.[9] The act also requires agencies to

[9]Under the Privacy Act of 1974, the term routine use means (with respect to the disclosure of a record) the use of a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

define—and limit themselves to—specific purposes for collecting the information.[10]

The Fair Information Practices, which form the basis of the Privacy Act, are a set of principles for protecting the privacy and security of personal information that were first proposed in 1973 by a U.S. government advisory committee.[11] These principles were intended to address what the committee considered the poor level of protection then being afforded to privacy under contemporary law. Since that time, the Fair Information Practices have been widely adopted as a benchmark for evaluating the adequacy of privacy protections. Appendix II contains a summary of the Fair Information Practices.

Preparing and issuing reports

The Homeland Security Act requires the Privacy Office to prepare annual reports to Congress detailing the department's activities affecting privacy, including complaints of privacy violations and implementation of the Privacy Act of 1974. In addition to the reporting requirements under the Homeland Security Act, Congress has occasionally directed the Privacy Office to report on specific technologies and programs. For example, in the conference report for the DHS appropriations act for fiscal year 2005, Congress directed the Privacy Office to report on DHS's use of data mining technologies.[12] Congress asked for a follow-up report on data mining in the conference report for the fiscal year 2007 DHS appropriations bill.[13] The Intelligence Reform and Terrorism Prevention Act of 2004 also required the Chief Privacy Officer to submit a report to Congress on the privacy and civil liberties impact of the DHS-maintained Automatic Selectee and No-Fly lists, which contain names of potential airline passengers who are to be selected for secondary screening or not allowed to board aircraft. In

[10]Agencies are allowed to claim exemptions from provisions of the Privacy Act if the records are used for specific purposes, such as law enforcement. 5 U.S.C. § 552a(j)&(k).

[11]Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973).

[12]Conference Report on H.R. 4567, Department of Homeland Security Appropriations Act, 2005, House Report 108-774 (Oct. 9, 2004).

[13]Conference Report on H.R. 5441, Department of Homeland Security Appropriations Act, 2007, House Report 109-699 (Sept. 28, 2006).

addition, the Privacy Office can initiate its own investigations and produce reports under its Homeland Security Act authority to report on complaints of privacy violations and assure technologies sustain and do not erode privacy protections.

DHS Privacy Office Has Made Significant Progress Establishing Processes to Ensure Implementation of Privacy Protections, but More Work Remains

The DHS Privacy Office has made significant progress in addressing its statutory responsibilities under the Homeland Security Act by developing processes to ensure implementation of privacy protections in departmental programs. For example, the Privacy Office has established processes for ensuring departmental compliance with the PIA requirement in the E-Gov Act of 2002. Instituting this framework has led to increased attention to privacy requirements on the part of departmental components, contributing to an increase in the quality and number of PIAs issued.

The Privacy Office has addressed its mandate to assure that technologies sustain, and do not erode, privacy protections through a variety of actions, including implementing its PIA compliance framework, establishing a federal advisory committee, raising awareness of privacy issues through a series of public workshops, and participating in policy development for several major DHS initiatives. The office has also taken action to address its mandate to evaluate regulatory and legislative proposals involving the use of personal information by the federal government and has coordinated with the DHS Officer for Civil Rights and Civil Liberties.

While substantial progress has been made in these areas, limited progress has been made in other important aspects of privacy protection. For example, while the Privacy Office has reviewed, approved, and issued 56 new and revised Privacy Act system-of-records notices since its establishment, little progress has been made in updating notices for legacy systems of records—older systems of records that were originally developed by other agencies prior to the creation of DHS. Because many of these notices are not up-to-date, the department is not in compliance with OMB requirements that system-of-records notices be reviewed biennially, nor can it be assured that the privacy implications of its many systems that process and maintain personal information have been fully and accurately disclosed to the public.

Further, the Privacy Office has generally not been timely in issuing public reports, potentially limiting their value and impact. The Homeland Security Act requires that the Privacy Office report annually to Congress on department activities that affect privacy, including complaints of privacy violations. However, the office has issued only two annual reports within

the 3-year period since it was established in April 2003, and one of these did not include complaints of privacy violations as required. In addition, required reports on several specific topics have also been late. In addition, the office initiated its own investigations of specific programs and produced reports on these reviews, several of which were not publicly released until long after concerns had been addressed. Late issuance of reports has a number of negative consequences beyond failure to comply with mandated deadlines, including a potential reduction in the reports' value and erosion of the office's credibility.

The Privacy Office Has Made Significant Progress in Reviewing and Approving PIAs, but Faces an Increasing Workload

One of the Privacy Office's primary responsibilities is to review and approve DHS PIAs, thus ensuring departmental compliance with the privacy provisions (section 208) of the E-Gov Act of 2002. The E-Gov Act requires that federal agencies perform PIAs before developing or procuring technology that collects, maintains, or disseminates personally identifiable information, or when initiating a new collection of personally identifiable information using information technology. In addition, the Homeland Security Act also specifically directs the office to perform PIAs for proposed departmental rules concerning the privacy of personal information. Further, the Privacy Office's involvement in the PIA process also addresses its broad Homeland Security Act requirement to "assure that technology sustains and does not erode privacy protections."

The Privacy Office Has Established a PIA Compliance Framework

The centerpiece of the Privacy Office's compliance framework is its written guidance on when a PIA must be conducted, how the associated analysis should be performed, and how the final document should be written. Although based on OMB's guidance,[14] the Privacy Office's guidance goes further in several areas. For example, the guidance does not exempt national security systems[15] and also clarifies that systems in the pilot testing phase are not exempt. The DHS guidance also provides more detailed instructions than OMB's guidance on the level of detail to be

[14]OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

[15]A national security system is defined by the Clinger-Cohen Act as an information system operated by the federal government, the function, operation, or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons system, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management.

provided. For example, the DHS guidance requires a discussion of a system's data retention period, procedures for allowing individual access, redress, correction of information, and technologies used in the system, such as biometrics or RFID.

The Privacy Office has taken steps to continually improve its PIA guidance. Initially released in February 2004, the guidance has been updated twice, in July 2005 and March 2006. These updates have increased the emphasis on describing the privacy analysis that should take place in making system design decisions that affect privacy. For example, regarding data retention, the latest guidance requires program officials to explain why the personal information in question is needed for the specified retention period. Based on feedback from DHS components, the Privacy Office plans to update the guidance again in 2007 to clarify questions on data mining and the use of commercial data. To accompany its written guidance, the Privacy Office has also developed a PIA template and a number of training sessions to further assist DHS personnel.

In addition to written guidance and training, the office developed a procedure, called a privacy threshold analysis (PTA), for identifying which DHS systems contain personally identifiable information and which require PIAs. The privacy threshold analysis is a brief assessment that requires system owners to answer six basic questions on the nature of their systems and whether the systems contain personally identifiable information. System owners complete the privacy threshold analysis document and submit it to the Privacy Office for an official determination as to whether a PIA is required. As of January 2006, all DHS systems have been required to perform privacy threshold analyses.

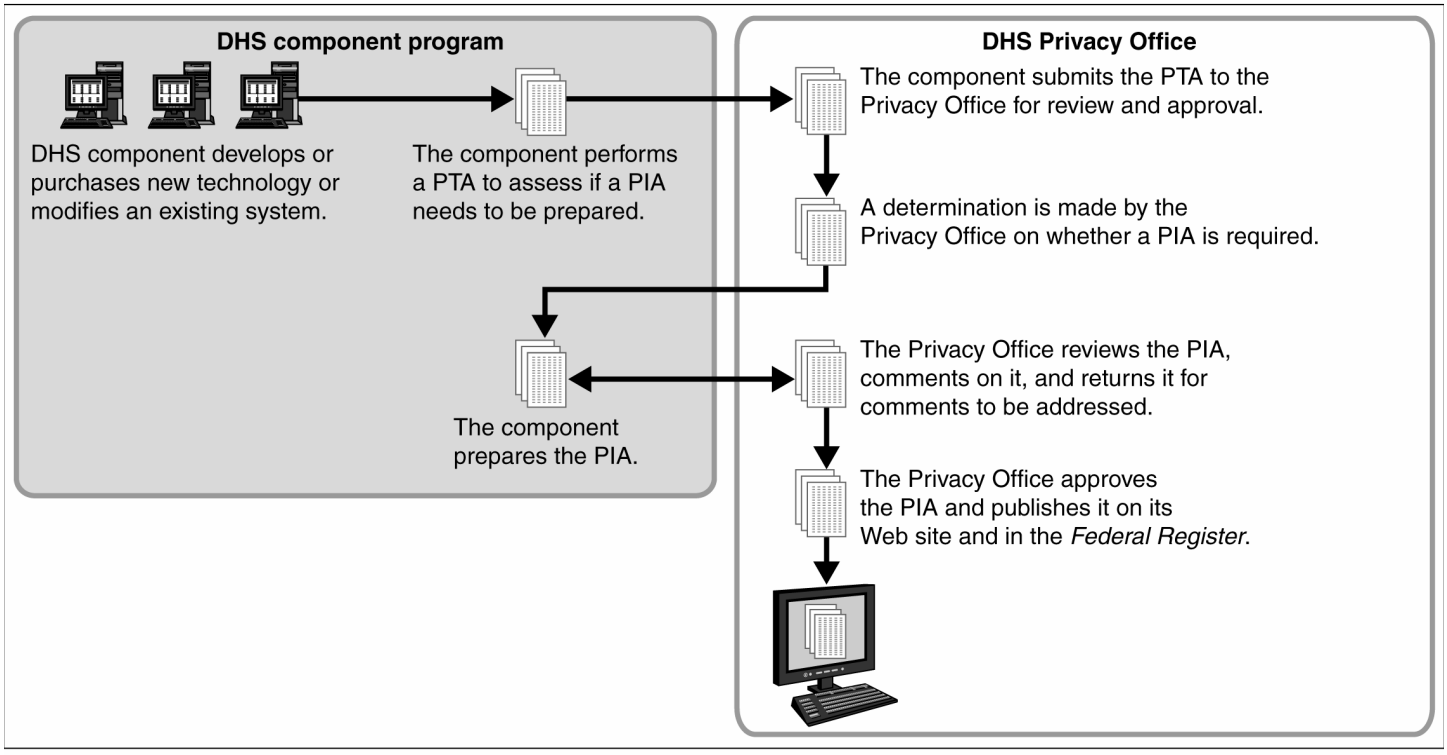
Our analysis of published DHS PIAs shows significant quality improvements in those completed recently compared with those from 2 or 3 years ago. Overall, there is a greater emphasis on analysis of system development decisions that impact privacy, because the guidance now requires that such analysis be performed and described. For example, the most recent PIAs include separate privacy impact analyses for several major topics, including planned uses of the system and information, plans for data retention, and the extent to which the information is to be shared outside of DHS. This contrasts to the earliest PIAs published by the Privacy Office, which do not include any of these analyses.

The emphasis on analysis should allow the public to more easily understand a system and its impact on privacy. Further, our analysis found that use of the template has resulted in a more standardized structure,

format, and content, making the PIAs more easily understandable to the general reader.

In addition to its positive impact on DHS, the Privacy Office's framework has been recognized by others outside of DHS. For example, the Department of Justice has adopted the DHS Privacy Office's guidance and template with only minor modifications. Further, privacy advocacy groups have commended the Privacy Office for developing the guidance and associated training sessions, citing this as one of the office's most significant achievements. Figure 2 illustrates the steps in the development process as established by the Privacy Office's guidance.

Figure 2: DHS PIA Development Process



Source: DHS.

The Privacy Office Has Integrated PIA Development into DHS Management Processes

In addition to written guidance, the Privacy Office has also taken steps to integrate PIA development into the department's established operational processes. For example, the Privacy Office coordinated with the Office of the Chief Information Officer (OCIO) to include the privacy threshold

analysis requirement as part of OCIO's effort to compile an inventory of major information systems required by the Federal Information Security Management Act.[16] Through this coordination, the Privacy Office was able to get the PTA requirement incorporated into the software application that DHS uses to track agency compliance with the Federal Information Security Management Act. The Privacy Office also coordinated with OCIO to include submission of a privacy threshold analysis as a requirement within the larger certification and accreditation process. The process requires IT system owners to evaluate security controls to ensure that security risks have been properly identified and mitigated. The actions they have taken are then scored, and systems must receive a certain minimum score in order to be certified and accredited.[17] The inclusion of the PTA as part of the systems inventory and in the certification and accreditation process has enabled the Privacy Office to better identify systems containing personally identifiable information that may require a PIA.

Further, the Privacy Office is using the OMB Exhibit 300 budget process[18] as an additional opportunity to ensure that systems containing personal information are identified and that PIAs are conducted when needed. OMB requires agencies to submit an Exhibit 300 Capital Asset Plan and Business Case for their major information technology systems in order to receive funding. The Exhibit 300 template asks whether a system has a PIA and if it is publicly available. Because the Privacy Office gives final departmental approval for all such assessments, it is able to use the Exhibit 300 process to ensure the assessments are completed. According to Privacy Office officials, the threat of losing funds has helped to encourage components to conduct PIAs. Integration of the PIA requirement into these management processes is beneficial in that it provides an opportunity to address

[16]The Federal Information Security Management Act establishes federal requirements for securing information and information systems that support federal agency operations and assets; it requires agencies to develop agencywide information security programs that extend to contractors and other providers of federal data and systems. Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

[17]An IT system must undergo certification and accreditation every 3 years to ensure that it is in compliance with OMB and National Institute of Standards and Technology guidance. For DHS systems, the completion of a privacy threshold analysis contributes to a system's overall certification and accreditation score.

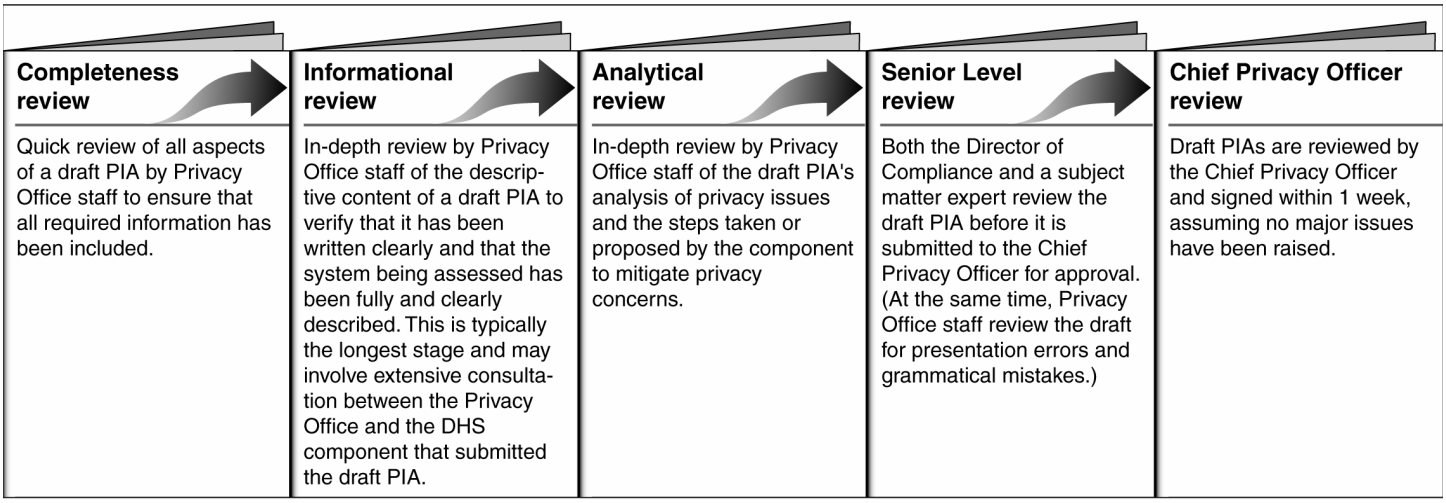
[18]OMB Circular No. A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets* (Washington, D.C.: June 2006).

privacy considerations during systems development, as envisioned by OMB's guidance.

The Privacy Office Is Taking Steps to Streamline PIA Review and Approval

Because of concerns expressed by component officials that the Privacy Office's review process took a long time and was difficult to understand, the office has made efforts to improve the process and make it more transparent to DHS components. Specifically, the office established a five-stage review process. Under this process, a PIA must satisfy all the requirements of a given stage before it can progress to the next one. The review process is intended to take 5 to 6 weeks, with each stage intended to take 1 week. Figure 3 illustrates the stages of the review process.

Figure 3: The PIA Review Process



Source: DHS.

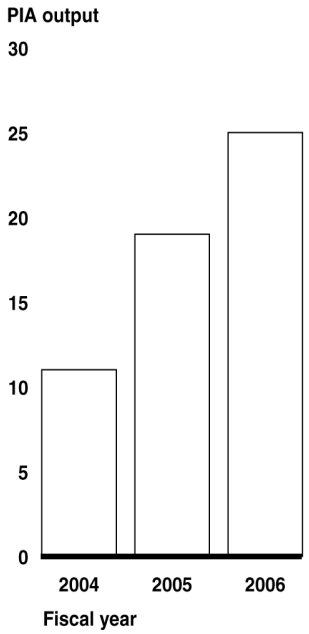
Privacy Office Efforts Have Helped to Identify the Need for an Increasing Number of PIAs

Through efforts such as the compliance framework, the Privacy Office has steadily increased the number of PIAs it has approved and published each year.[19] As shown in figure 4, PIA output by the Privacy Office has more than doubled since 2004. According to Privacy Office officials, the increase

[19]As of February 2007, the Privacy Office had approved and published a total of 71 PIAs. Of these, 46 were new, 20 were updates to preexisting documents, and 5 were PIAs for agency rules. Section 222 of the Homeland Security Act requires the Chief Privacy Officer to "[conduct] a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information including the type of personal information collected and the number of people affected."

in output was aided by the development and implementation of the Privacy Office's structured guidance and review process. In addition, Privacy Office officials stated that as DHS components gain more experience, the output should continue to increase.

Figure 4: Numbers of PIAs Published Annually for DHS Systems



Source: GAO analysis of published DHS PIAs.

Because the Privacy Office has focused departmental attention on the development and review process and established a structured framework for identifying systems that need PIAs, the number of identified DHS systems requiring a PIA has increased dramatically. According to its annual Federal Information Security Management Act reports, DHS identified 46 systems as requiring a PIA in fiscal year 2005 and 143 systems in fiscal year 2006. Based on the privacy threshold analysis process, the Privacy Office estimates that 188 systems will require a PIA in fiscal year 2007.

Considering that only 25 were published in fiscal year 2006, it will likely be very difficult for DHS to expeditiously develop and issue PIAs for all of these systems because developing and approving them can be a lengthy process. According to estimates by Privacy Office officials, it takes

approximately six months[20] to develop and approve a PIA, but the office is working to reduce this time.

The Privacy Office is examining several potential changes to the development process that would allow it to process an increased number of PIAs. One such option is to allow DHS components to quickly amend preexisting PIAs. An amendment would only need to contain information on changes to the system and would allow for quicker development and review. The Privacy Office is also considering developing standardized PIAs for commonly-used types of systems or uses. For example, such an assessment may be developed for local area networks. Systems intended to collect or use information outside what is specified in the standardized PIA would need approval from the Privacy Office.

Of potential help in dealing with an increasing PIA workload is the establishment of full-time privacy officers within key DHS components. Components with a designated privacy officer have generally produced more PIAs than components without privacy officers. Of the eleven DHS components that have published PIAs, only three have designated privacy officers. Yet these three components account for 57 percent of all published DHS PIAs.[21] Designating privacy officers in key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, Immigration and Customs Enforcement, and the Federal Emergency Management Agency, could help in drafting PIAs that could be processed by the Privacy Office more expeditiously. Components such as these have a high volume of programs that interface directly with the public. Although the Privacy Office has also recommended that such privacy officers be designated, the department has not yet appointed privacy officers in any of these components. Until DHS does so, the Privacy Office will likely continue to be challenged in ensuring that PIAs are prepared, reviewed, and approved in a timely fashion.

[20]Although PIA development time is not formally tracked, DHS component-level officials reported it could take significantly longer than 6 months to develop a PIA.

[21]Of the DHS components that have published PIAs, three have designated privacy officers: TSA, the US-VISIT program, and the U.S. Citizenship and Immigration Services.

The Privacy Office Has Taken Steps to Integrate Privacy Into DHS Decision Making

The Privacy Office has also taken steps to integrate privacy considerations in the DHS decision-making process. These actions are intended to address a number of statutory requirements, including that the Privacy Office assure that the use of technologies sustain, and do not erode, privacy protections; that it evaluate legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government; and that it coordinate with the DHS Officer for Civil Rights and Civil Liberties.

The Data Privacy and Integrity Advisory Committee Was Established to Provide Outside Advice

In 2004, the first Chief Privacy Officer established the DHS Data Privacy and Integrity Advisory Committee to advise her and the Secretary on issues within the department that affect individual privacy, as well as data integrity, interoperability, and other privacy-related issues. The committee has examined a variety of privacy issues, produced reports, and made recommendations. Most recently, in December 2006, the committee adopted two reports; one on the use of RFID for identity verification, and another on the use of commercial data. As previously mentioned, the Privacy Office plans to update its PIA guidance to include further instructions on the use of commercial data. According to Privacy Office officials, this update will be based, in part, on the advisory committee's report on commercial data. Appendix III contains a full list of the advisory committee's publications.

In addition to its reports, which are publicly available, the committee meets quarterly in Washington, D.C., and in other parts of the country where DHS programs operate. These meetings are open to the public and transcripts of the meetings are posted on the Privacy Office's Web site.[22] DHS officials from major programs and initiatives involving the use of personal data such as US-VISIT, Secure Flight, and the Western Hemisphere Travel Initiative, have testified before the committee. Private sector officials have also testified on topics such as data integrity, identity authentication, and RFID.

Because the committee is made up of experts from the private sector and the academic community, it brings an outside perspective to privacy issues through its reports and recommendations. In addition, because it was established as a federal advisory committee, its products and proceedings

[22]Reports produced by the DHS Data Privacy and Integrity Advisory Committee and transcripts of quarterly meetings can be found at http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm.

are publicly available and thus provide a public forum for the analysis of privacy issues that affect DHS operations.

Privacy Office Workshops Have Highlighted Key Issues

The Privacy Office has also taken steps to raise awareness of privacy issues by holding a series of public workshops. The first workshop, on the use of commercial data for homeland security, was held in September 2005. Panel participants consisted of representatives from academia, the private sector, and government. In April 2006, a second workshop addressed the concept of public notices and freedom of information frameworks. More recently, in June 2006, a workshop was held on the policy, legal, and operational frameworks for PIAs and privacy threshold analyses and included a tutorial for conducting PIAs.[23] Hosting public workshops is beneficial in that it allows for communication between the Privacy Office and those who may be affected by DHS programs, including the privacy advocacy community and the general public.

Privacy Office Officials Have Participated in the DHS Decision-making Process

Another part of the Privacy Office's efforts to carry out its Homeland Security Act requirements is its participation in departmental policy development for initiatives that have a potential impact on privacy. The Privacy Office has been involved in policy discussions related to several major DHS initiatives and, according to department officials, the office has provided input on several privacy-related decisions. The following are major initiatives in which the Privacy Office has participated.

Passenger name record negotiations with the European Union

United States law requires airlines operating flights to or from the United States to provide the Bureau of Customs and Border Protection (CBP) with certain passenger reservation information for purposes of combating terrorism and other serious criminal offenses.[24] In May 2004, an international agreement on the processing of this information was signed by DHS and the European Union.[25] Prior to the agreement, CBP established a set of terms for acquiring and protecting data on European

[23]In addition, in November 2006, the Privacy Office, US-VISIT program, and the DHS Biometrics Coordination Group sponsored a conference on privacy issues related to biometric technology; however, this conference was not open to the public or the media.

[24]49 U.S.C. Chapter 449.

[25]The EU Data Protection Directive (Article 25(6) of Directive 95/46/EC) generally prohibits cross-border sharing with non-EU countries unless the receiving entity demonstrates that it has adequate data protection standards.

Union citizens, referred to as the "Undertakings."[26] In September 2005, under the direction of the first Chief Privacy Officer, the Privacy Office issued a report on CBP's compliance with the Undertakings in which it provided guidance on necessary compliance measures and also required certain remediation steps. For example, the Privacy Office required CBP to review and delete data outside the 34 data elements permitted by the agreement. According to the report, the deletion of these extraneous elements was completed in August 2005 and was verified by the Privacy Office.

In October 2006, DHS and the European Union completed negotiations on a new interim agreement concerning the transfer and processing of passenger reservation information. The Director of International Privacy Policy within the Privacy Office participated in these negotiations along with others from DHS in the Policy Office, Office of General Counsel, and CBP.

Western Hemisphere Travel Initiative

The Western Hemisphere Travel Initiative is a joint effort between DHS and the Department of State to implement new documentation requirements for certain U.S. citizens and nonimmigrant aliens entering the United States. DHS and State have proposed the creation of a special identification card that would serve as an alternative to a traditional passport for use by U.S. citizens who cross land borders or travel by sea between the United States, Canada, Mexico, the Caribbean, or Bermuda.[27] The card is to use a technology called vicinity RFID to transmit information on travelers to CBP officers at land and sea ports of entry. Advocacy groups have raised concerns about the proposed use of vicinity RFID because of privacy and security risks due primarily to the ability to read information from these cards from distances of up to 20 feet. The Privacy Office was consulted on the choice of identification technology for the cards. According to the DHS Policy Office, Privacy Office input led to a decision not to store or transmit personally identifiable information on the RFID chip on the card. Instead, DHS is planning on transmitting a randomly generated identifier for individuals, which is to be used by DHS to retrieve information about the individual from a centralized database.

[26]DHS Privacy Office, *A Report Concerning Passenger Name Record Information Derived From Flights Between the U.S. and The European Union* (Sept. 19, 2005).

[27]71 *Federal Register* 60928-60932 (Oct. 17, 2006).

REAL ID Act of 2005

Among other things, the REAL ID Act[28] requires DHS, in consultation with the Department of Transportation and the states, to issue regulations that set minimum standards for state-issued REAL ID drivers' licenses and identification cards to be accepted for official purposes after May 11, 2008. Advocacy groups have raised a number of privacy concerns about REAL ID, chiefly that it creates a de facto national ID that could be used in the future for privacy-infringing purposes and that it puts individuals at increased risk of identity theft. The DHS Policy Office reported that it included Privacy Office officials, as well as officials from the Office of Civil Rights and Civil Liberties, in developing its implementing rule for REAL ID.[29] The Privacy Office's participation in REAL ID also served to address its requirement to evaluate legislative and regulatory proposals concerning the collection, use, and disclosure of personal information by the federal government.[30] According to its November 2006 annual report, the Privacy Office championed the need for privacy protections regarding the collection and use of the personal information that will be stored on the REAL ID drivers' licenses. Further, the office reported that it funded a contract to examine the creation of a state federation to implement the information sharing required by the act in a privacy-sensitive manner.

Use of commercial data

As we have previously reported, DHS has used personal information obtained from commercial data providers for immigration, fraud detection, and border screening programs but, like other agencies, does not have policies in place concerning its uses of these data.[31] Accordingly, we recommended that DHS, as well as other agencies, develop such

[28]Division B, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13 (May 11, 2005).

[29]The Intelligence Reform Act of 2004 requires the DHS Privacy Officer to coordinate activities with the DHS Officer for Civil Rights and Civil Liberties. Participation in this working group is one example of coordination between the two offices.

[30]Privacy Office officials reported that they use the OMB legislative review process and the publication of rules in the *Federal Register* as mechanisms for reviewing emerging rules and legislation. In addition, the Privacy Office recently created a Director of Legislative and Regulatory Affairs position to coordinate, among other things, review of proposed privacy legislation and rulemakings. This position was filled in February 2007.

[31]GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

policies. In response to the concerns raised in our report and by privacy advocacy groups, Privacy Office officials said they were drafting a departmentwide policy on the use of commercial data. Once drafted by the Privacy Office, this policy is to undergo a departmental review process (including review by the Policy Office, General Counsel, and Office of the Secretary), followed by a review by OMB prior to adoption.

These examples demonstrate specific involvement of the Privacy Office in major DHS initiatives. However, Privacy Office input is only one factor that DHS officials consider in formulating decisions about major programs, and Privacy Office participation does not guarantee that privacy concerns will be fully addressed. For example, our previous work has highlighted problems in implementing privacy protections in specific DHS programs, including Secure Flight[32] and the ADVISE program.[33] Nevertheless, the Privacy Office's participation in policy decisions provides an opportunity for privacy concerns to be raised explicitly and considered in the development of DHS policies.

The Privacy Office Has Coordinated Activities with the DHS Officer for Civil Rights and Civil Liberties

The Privacy Office has also taken steps to address its mandate to coordinate with the DHS Officer for Civil Rights and Civil Liberties on programs, policies, and procedures that involve civil rights, civil liberties, and privacy considerations, and ensure that "Congress receives appropriate reports on such programs." The DHS Officer for Civil Rights and Civil Liberties cited three specific instances where the offices have collaborated. First, as stated previously, both offices have participated in the working group involved in drafting the implementing regulations for REAL ID. Second, the two offices coordinated in preparing the Privacy Office's report to Congress assessing the privacy and civil liberties impact of the No-Fly and Selectee lists used by DHS for passenger prescreening. Third, the two offices coordinated on providing input for the "One-Stop Redress" initiative, a joint initiative between the Department of State and DHS to implement a streamlined redress center for travelers who have concerns about their treatment in the screening process.

[32]GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

[33]GAO, *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*, GAO-07-293 (Washington, D.C.: Feb. 28, 2007).

Although Privacy Act Processes Have Been Established, Little Progress Has Been Made in Updating Public Notices for DHS Legacy Systems-of-Records

The DHS Privacy Office is responsible for reviewing and approving DHS system-of-records notices to ensure that the department complies with the Privacy Act of 1974. Specifically, the Homeland Security Act requires the Privacy Office to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." The Privacy Act requires that federal agencies publish notices in the *Federal Register* on the establishment or revision of systems of records. These notices must describe the nature of a system-of-records and the information it maintains. Additionally, OMB has issued various guidance documents for implementing the Privacy Act. OMB Circular A-130, for example, outlines agency responsibilities for maintaining records on individuals and directs government agencies to conduct biennial reviews of each system-of-records notice to ensure that it accurately describes the system-of-records.[34]

The Privacy Office has taken steps to establish a departmental process for complying with the Privacy Act. It issued a management directive that outlines its own responsibilities as well as those of component-level officials. Under this policy, the Privacy Office is to act as the department's representative for matters relating to the Privacy Act. The Privacy Office is to issue and revise, as needed, departmental regulations implementing the Privacy Act and approve all system-of-records notices before they are published in the *Federal Register*. DHS components are responsible for drafting system-of-records notices and submitting them to the Privacy Office for review and approval. The management directive was in addition to system-of-records notice guidance published by the Privacy Office in August 2005. The guidance discusses the requirements of the Privacy Act and provides instructions on how to prepare system-of-records notices by listing key elements and explaining how they must be addressed. The guidance also lists common routine uses and provides standard language that DHS components may incorporate into their notices. As of February 2007, the Privacy Office had approved and published 56 system-of-records notices, including updates and revisions as well as new documents.

In establishing Privacy Act processes, the Privacy Office has also begun to integrate the system-of-records notice and PIA development processes. The Privacy Office now generally requires that system-of-records notices

[34]OMB, *Management of Federal Information Resources*, Circular A-130, Appendix 1 (Nov. 28, 2000).

submitted to it for approval be accompanied by PIAs. This is not an absolute requirement, because the need to conduct PIAs, as stipulated by the E-Gov Act, is not based on the same concept of a "system-of-records" used by the Privacy Act. Nevertheless, the Privacy Office's intention is to ensure that, when the requirements do coincide, a system's PIA is aligned closely with the related system-of-records notice.

However, the Privacy Office has not yet established a process for conducting a biennial review of system-of-records notices, as required by OMB. OMB Circular A-130 directs federal agencies to review their notices biennially to ensure that they accurately describe all systems of records. Where changes are needed, the agencies are to publish amended notices in the *Federal Register*.[35]

The establishment of DHS involved the consolidation of a number of preexisting agencies, thus, there are a substantial number of systems that are operating under preexisting, or "legacy," system-of-records notices—218, as of February 2007. [36] These documents may not reflect changes that have occurred since they were prepared. For example, the system-of-records notice for the Treasury Enforcement and Communication System has not been updated to reflect changes in how personal information is used that has occurred since the system was taken over by DHS from the Department of the Treasury.

The Privacy Office acknowledges that identifying, coordinating, and updating legacy system-of-records notices is the biggest challenge it faces in ensuring DHS compliance with the Privacy Act. Because it focused its initial efforts on PIAs and gave priority to DHS systems of records that were not covered by preexisting notices, the office did not give the same priority to performing a comprehensive review of existing notices. According to Privacy Office officials, the office is encouraging DHS components to update legacy system-of-records notices and is developing new guidance intended to be more closely integrated with its PIA guidance. However, no significant reduction has yet been made in the number of legacy system-of-records notices that need to be updated.

[35]OMB gives agencies the option to publish one annual comprehensive publication consolidating minor changes.

[36]DHS system-of-records are covered by preexisting notices through the operation of a savings provision in the Homeland Security Act of 2002. 6 U.S.C. § 552.

By not reviewing notices biennially, the department is not in compliance with OMB direction. Further, by not keeping its notices up-to-date, DHS hinders the public's ability to understand the nature of DHS systems-of-records notices and how their personal information is being used and protected. Inaccurate system-of-records notices may make it difficult for individuals to determine whether their information is being used in a way that is incompatible with the purpose for which it was originally collected.

Privacy Office Has Generally Not Issued Reports in a Timely Fashion

Section 222 of the Homeland Security Act requires that the Privacy Officer report annually to Congress on "activities of the department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters." The act does not prescribe a deadline for submission of these reports; however, the requirement to report "on an annual basis" suggests that each report should cover a 1-year time period and that subsequent annual reports should be provided to Congress 1 year after the previous report was submitted. Congress has also required that the Privacy Office report on specific departmental activities and programs, including data mining and passenger prescreening programs. In addition, the first Chief Privacy Officer initiated several investigations and prepared reports on them to address requirements to report on complaints of privacy violations and to assure that technologies sustain and do not erode privacy protections.

In addition to satisfying mandates, the issuance of timely public reports helps in adhering to the fair information practices, which the Privacy Office has pledged to support. Public reports address openness—the principle that the public should be informed about privacy policies and practices and that individuals should have a ready means of learning about the use of personal information—and the accountability principle—that individuals controlling the collection or use of personal information should be accountable for taking steps to ensure implementation of the fair information principles.

The Privacy Office has not been timely and in one case has been incomplete in addressing its requirement to report annually to Congress. The Privacy Office's first annual report, issued in February 2005, covered 14 months from April 2003 through June 2004. A second annual report, for the next 12 months, was never issued. Instead, information about that period was combined with information about the next 12-month period, and a single report was issued in November 2006 covering the office's activities from July 2004 through July 2006. While this report generally

addressed the content specified by the Homeland Security Act, it did not include the required description of complaints of privacy violations.

Other reports produced by the Privacy Office have not met mandated deadlines or have been issued long after privacy concerns had been addressed. For example, although Congress required a report on the privacy and civil liberties effects of the No-Fly and Automatic Selectee Lists[37] by June 2005, the report was not issued until April 2006, nearly a year late. In addition, although required by December 2005, the Privacy Office's report on DHS data mining activities was not provided to Congress until July 2006 and was not made available to the public on the Privacy Office Web site until November 2006.

In addition, the first Chief Privacy Officer initiated four investigations of specific programs and produced reports on these reviews. Although two of the four reports were issued in a relatively timely fashion, the other two reports were issued long after privacy concerns had been raised and addressed. For example, a report on the Multi-state Anti-Terrorism Information Exchange (MATRIX) program, initiated in response to a complaint by the American Civil Liberties Union submitted in May 2004, was not issued until two and a half years later, long after the program had been terminated. As another example, although drafts of the recommendations contained in the Secure Flight report were shared with TSA staff as early as summer 2005, the report was not released until December 2006, nearly a year and a half later. Table 1 summarizes DHS Privacy Office reports issued to date, including both statutorily required as well as self-initiated reports.

[37]These lists are used by TSA and CBP for screening airline and cruise line passengers. Individuals on the lists may be denied boarding or selected for additional screening.

Table 1: Summary of DHS Privacy Office Reports by Date Released

Report	Description	Date released
Report to the Public on the Events Surrounding the jetBlue Data Transfer	This report provides the results of a study initiated in September 2003 in response to a potential privacy violation by TSA that took place in 2001 and 2002, prior to TSA becoming a part of DHS. The incident involved the transfer of passenger name records from jetBlue Airways to the Department of Defense, a transfer that occurred with involvement by TSA personnel. The report presented findings on the incident and offers recommendations including that TSA employees attend comprehensive privacy training and that DHS establish guidelines for data sharing, including sharing with the private sector for security purposes.	February 2004
First annual report	This report, required by Section 222 of the Homeland Security Act, discusses Privacy Office activities from April 2003 though June 2004. Among other things, the report describes the establishment of the Privacy Office as well as actions to comply with statutory requirements including efforts to implement the PIA requirement and ensure compliance with the Privacy Act. The report also describes complaints of privacy violations as required by the Homeland Security Act, including those related to the Computer Assisted Passenger Prescreening II program, the transfer of passenger name record data from jetBlue to the Department of Defense, and the Multi-State Anti-Terrorism Information Exchange program.	February 2005
Second annual report	This report was drafted but never released. The content of this report was merged with that of the third annual report.	No report issued—merged with third annual report
Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union	In May 2004, an international agreement regarding the processing of passenger name records was signed by DHS and the European Union. Prior to the agreement, CBP established a set of terms by which these records were to be provided to and protected by CBP, referred to as the "Undertakings." The first Chief Privacy Officer initiated a review of CBP's compliance with representations made in the Undertakings in November 2004 and completed her review in September 2005. In the report, the Privacy Office found CBP generally in compliance with the Undertakings but also noted that during the course of the review, areas for improvement were identified to achieve fuller compliance. The Privacy Office provided guidance on necessary compliance measures and also required certain remediation steps. For example, the Privacy Office required CBP to review and delete data outside the 34 data elements permitted by the agreement.	September 19, 2005
Impact of the Automatic Selectee & No Fly List on Privacy & Civil Liberties	Section 4012(b)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 required the DHS Privacy Officer to prepare and submit a report to Congress by June 2005 assessing the impact of the Automatic Selectee and No-Fly lists on privacy and civil liberties. These lists are used by TSA and CBP for screening airline and cruise line passengers. Individuals on the lists may be denied boarding or selected for additional screening.	April 27, 2006

Report	Description	Date released
Data mining report	House Conference Report 108-774 on the DHS 2005 Appropriations Act required a report on DHS data mining activities by December 2005. This report catalogued DHS data mining activities and included descriptions of the purposes of the programs; data sources; deployment dates; and policies, procedures, and guidance. The report includes a number of recommendations aimed at mitigating the privacy risks associated with data mining. In the fiscal year 2007 DHS appropriations conference report, Congress required the Privacy Office to report again on DHS data mining activities, including progress made in implementing the July 2006 report's recommendations.	Congress: July 6, 2006 Public: November 29, 2006
Third annual report	This report covers the Privacy Office's activities from July 2004 through July 2006. The report describes its efforts to "build a culture of privacy attentiveness at DHS," a discussion of responding to national and global challenges and a review of outreach efforts such as public workshops and Data Privacy and Integrity Advisory Committee meetings. The report does not contain a discussion of complaints of privacy violations, as required by the Homeland Security Act.	Congress: November 17, 2006 Public: November 28, 2006
Secure Flight report	This is the final report on an investigation initiated by the first Chief Privacy Officer in response to concerns raised by GAO about Secure Flight commercial data testing in June 2005. The Privacy Office found that the commercial data test conducted in connection with the Secure Flight program did not match TSA's public announcements. The report offers a number of recommendations for the Secure Flight program.	December 22, 2006
MATRIX	The MATRIX program pilot project was a "proof of concept" initiated in response to the need for information sharing within state law enforcement communities and was funded through grants by the Department of Justice and DHS. The project used information technology as a means to more quickly access, share, and analyze public records to assist law enforcement. The first Chief Privacy Officer initiated a review of the MATRIX pilot project, to which DHS contributed funding, in response to a May 2004 complaint by the American Civil Liberties Union. This investigation was announced in the Privacy Office's first annual report (covering April 2003-July 2004) and states that the results of the MATRIX program report "will be made public in the near future in a forthcoming report." Although the report was not issued until December 2006, the MATRIX program had been effectively ended in April 2005. The report concludes that the MATRIX program pilot project lost public support because it failed to consider and adopt comprehensive privacy protections from the beginning. Although the program was already defunct, the Privacy Office offered recommendations as "lessons learned."	December 22, 2006

Source: GAO analysis of DHS Privacy Office reports.

According to Privacy Office officials, there are a number of factors contributing to the delayed release of its reports, including time required to consult with affected DHS components as well as the departmental clearance process, which includes the Policy Office, the Office of General Counsel, and the Office of the Secretary. After that, drafts must be sent to OMB for further review. In addition, the Privacy Office did not establish

schedules for completing these reports that took into account the time needed for coordination with components or departmental and OMB review.

Regarding the omission of complaints of privacy violations in the latest annual report, Privacy Office officials noted that the report cites previous reports on Secure Flight and the MATRIX program, which were initiated in response to alleged privacy violations, and that during the time period in question there were no additional complaints of privacy violations. However, the report itself provides no specific statements about the status of privacy complaints; it does not state that there were no privacy complaints received.

Late issuance of reports has a number of negative consequences beyond noncompliance with mandated deadlines. First, the value these reports are intended to provide is reduced when the information contained is no longer timely or relevant. In addition, since these reports serve as a critical window into the operations of the Privacy Office and on DHS programs that make use of personal information, not issuing them in a timely fashion diminishes the office's credibility and can raise questions about the extent to which the office is receiving executive-level attention. For example, delays in releasing the most recent annual report led a number of privacy advocates to question whether the Privacy Office had adequate authority and executive-level support. Congress also voiced this concern in passing the Department of Homeland Security Appropriations Act of 2007, which states that none of the funds made available in the act may be used by any person other than the Privacy Officer to "alter, direct that changes be made to, delay, or prohibit the transmission to Congress" of its annual report.[38] In addition, on January 5, 2007, legislation was introduced entitled Privacy Officer with Enhanced Rights Act of 2007. This bill, among other things, would provide the Privacy Officer with the authority to report directly to Congress without prior comment or amendment by either OMB officials or DHS officials who are outside the Privacy Office.[39] Until its

[38]Department of Homeland Security Appropriations Act, 2007 (Pub. L. 109-295). The President's signing statement to that act stated, among other things, "the executive branch shall construe section 522 of the act, relating to privacy officer reports, in a manner consistent with the President's constitutional authority to supervise the unitary executive branch."

[39]Subtitle B of Tile VIII of H.R. 1, "Implementing the 9/11 Commission Recommendations Act of 2007," introduced on January 5, 2007. The legislation also grants the Privacy Officer investigative authority, including subpoena power.

reports are issued in a timely fashion, questions about the credibility and authority of the Privacy Office will likely remain.

Conclusions

The DHS Privacy Office has made significant progress in implementing its statutory responsibilities under the Homeland Security Act; however, more work remains to be accomplished. The office has made great strides in implementing a process for developing PIAs, contributing to greater output over time and higher quality assessments. The Privacy Office has also provided the opportunity for privacy to be considered at key stages in systems development by incorporating PIA requirements into existing management processes. However, the Privacy Office faces a difficult task in reviewing and approving PIAs in a timely fashion for the large number of systems that require them. Component-level privacy officers could help coordinate processing of PIAs. Until DHS appoints such officers, the Privacy Office will not benefit from their potential to help speed the processing of PIAs.

Although the Privacy Office has made progress publishing new and revised Privacy Act notices since its establishment, privacy notices for DHS legacy systems of records have generally not been updated. The Privacy Office has not made it a priority to address the OMB requirement that existing notices be reviewed biennially. Until DHS reviews and updates its legacy notices as required by federal guidance, it cannot assure the public that its notices reflect current uses and protections of personal information.

Further, the Privacy Office has not issued reports in a timely fashion, and its most recent annual report did not address all of the content specified by the Homeland Security Act, which requires the office to report on complaints of privacy violations. There are a number of factors contributing to the delayed release of its reports, including time required to consult with affected DHS components as well as the departmental clearance process, and there is no schedule for reviews to be completed and final reports issued. Late issuance of reports has a number of negative consequences beyond failure to comply with mandated deadlines, such as a perceived and real reduction in their value, a reduction in the office's credibility, and the perception that the office lacks executive-level support. Until DHS develops a schedule for the timely issuance of reports, these negative consequences are likely to continue.

Recommendations for Executive Action

We recommend that the Secretary of Homeland Security take the following four actions:

- Designate full-time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, Immigration and Customs Enforcement, and the Federal Emergency Management Agency.
- Implement a department-wide process for the biennial review of system-of-records notices, as required by OMB.
- Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report development, including departmental clearance.
- Ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the DHS Departmental GAO/Office of Inspector General Liaison Office, which are reproduced in appendix IV. In its comments, DHS generally agreed with the content of the draft report and its recommendations and described actions initiated to address them.

In its comments, DHS stated that it appreciated GAO's acknowledgement of its success in creating a standardized process for developing privacy compliance documentation for individual systems and managing the overall compliance process. DHS also stated that it appreciated recognition of the establishment of the DHS Data Privacy and Integrity Advisory Committee and the Privacy Office's public meetings and workshops. In addition, DHS provided additional information about the international duties of the Privacy Office, specifically its outreach efforts with the European Union and its participation in regional privacy groups such as the Organization for Economic Cooperation and Development (OECD) and the Asian Pacific Economic Cooperation forum. DHS also noted that it had issued its first policy guidance memorandum regarding handling of information on non-U.S. persons.

Concerning our first recommendation that it designate full-time privacy officers in key departmental components, DHS noted that the recommendation was consistent with a departmental management directive on compliance with the Privacy Act and stated that it would take the recommendation "under advisement." DHS noted that component privacy officers not only make contributions in terms of producing privacy

impact assessments, but also provide day-to-day privacy expertise within their components to programs at all stages of development.

DHS concurred with the other three recommendations and noted actions initiated to address them. Specifically, regarding our recommendation that DHS implement a process for the biennial review of system of records notices required by OMB, DHS noted that it is systematically reviewing legacy system-of-records notices in order to issue updated notices on a schedule that gives priority to systems with the most sensitive personally identifiable information. DHS also noted that the Privacy Office is to issue an updated system-of-records notice guide by the end of fiscal year 2007. Concerning our recommendation related to timely reporting, DHS stated that the Privacy Office will work with necessary components and programs affected by its reports to provide for both full collaboration and coordination within DHS. Finally, regarding our recommendation that the Privacy Office's annual reports contain a specific discussion of privacy complaints, as required by law, DHS agreed that a consolidated reporting structure for privacy complaints within the annual report would assist in assuring Congress and the public that the Privacy Office is addressing the complaints that it receives.

As agreed with your offices, 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 Secretary of Homeland Security and other interested congressional committees. Copies will be made available to others on request. In addition, this report will be available at no charge on our Web site at 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 V.

Linda D. Koontz
Director
Information Management Issues

List of Requesters

The Honorable Jerrold Nadler
Chairman
Subcommittee on the Constitution, Civil Rights, and Civil Liberties
Committee on the Judiciary
House of Representatives

The Honorable Chris Cannon
Ranking Member
Subcommittee on Commercial and Administrative Law
Committee on the Judiciary
House of Representatives

The Honorable Mel Watt
The Honorable Steve Chabot
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to assess the progress of the Department of Homeland Security (DHS) Privacy Office in carrying out its responsibilities under federal law, including the Homeland Security Act of 2002 and the E-Government Act of 2002.

To address this objective, we analyzed the Privacy Office's enabling statutes, Section 222 of the Homeland Security Act; Section 8305 of the Intelligence Reform and Terrorism Prevention Act of 2004; and applicable federal privacy laws, including the Privacy Act of 1974 and Section 208 of the E-Government Act, to identify DHS Privacy Office responsibilities. We reviewed and analyzed Privacy Office policies, guidance, and reports, and interviewed Privacy Office officials, including the Chief Privacy Officer, the Acting Chief of Staff, and the Director of Privacy Compliance, to identify Privacy Office plans, priorities, and processes for implementing its responsibilities using available resources. We did not review or assess the Privacy Office's Freedom of Information Act responsibilities.

To further address our objective, we assessed the Privacy Office's progress by comparing the information we gathered with the office's statutory requirements and other responsibilities. We evaluated Privacy Office policies, guidance, and processes for ensuring compliance with the Homeland Security Act, the Privacy Act, and the E-Government Act. We analyzed the system-of-records notices and PIA development processes and assessed the progress of the office in implementing these processes. This analysis included analyzing Privacy Office privacy impact assessment output by fiscal year and assessing improvements to the overall quality of published privacy impact assessments and guidance over time.

In addition, we interviewed the DHS Officer for Civil Rights and Civil Liberties, component-level privacy officers at the Transportation Security Administration, US-Visitor and Immigrant Status Indicator Technology, and U.S. Citizenship and Immigration Services, and cognizant component-level officials from Customs and Border Protection, Immigration and Customs Enforcement, and the DHS Policy Office. We also interviewed former DHS Chief Privacy Officers; the chair and vice-chair of the DHS Data Privacy and Integrity Advisory Committee, and privacy advocacy groups, including the American Civil Liberties Union, the Center for Democracy and Technology, and the Electronic Privacy Information Center.

We performed our work at the DHS Privacy Office in Arlington, Virginia, and major DHS components in the Washington, D.C., metropolitan area. In addition, we attended DHS Data Privacy and Integrity Advisory Committee

public meetings in Arlington, Virginia, and Miami, Florida. Our work was conducted from June 2006 to March 2007 in accordance with generally accepted government auditing standards.

Appendix II: The Fair Information Practices

The Fair Information Practices are not precise legal requirements. Rather, they provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. Ways to strike that balance vary among countries and according to the type of information under consideration. The version of the Fair Information Practices shown in table 1 was issued by the Organization for Economic Cooperation and Development (OECD) in 1980[1] and it has been widely adopted.

Table 2: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and on any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

[1]OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). The OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

Appendix III: Department of Homeland Security Data Privacy and Integrity Advisory Committee Publications

The Use of Commercial Data. Report No. 2006-03. December 6, 2006.

The Use of RFID for Human Identity Verification. Report No. 2006-02. December 6, 2006.

Framework for Privacy Analysis of Programs, Technologies, and Applications. Report No. 2006-01. March 7, 2006.

Recommendations on the Secure Flight Program. Report No. 2005-02. December 6, 2005.

The Use of Commercial Data to Reduce False Positives in Screening Programs. Report No. 2005-01. September 28, 2005.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 12, 2007

Ms. Linda D. Koontz
Director, Information Management Issues
General Accountability Office
Washington, DC 20548

Dear Ms. Koontz:

RE: Draft Report GAO-07-522, DHS Privacy Office: Progress Made But Challenges Remain in Notifying and Reporting to the Public

Thank you for the opportunity to review the draft report. In this draft report, the Government Accountability Office (GAO) highlights the accomplishments of the Department of Homeland Security (DHS) Privacy Office (Privacy Office) and makes four recommendations for the Privacy Office in moving forward with its mission.

This draft report constitutes GAO's first review of a statutory privacy office in a federal agency and the Privacy Office's privacy responsibilities for a newly created agency composed of over 180,000 employees and 22 components brought together from a number of separate government agencies. When the Privacy Office stood up four years ago with the rest of DHS, it took on the unprecedented responsibility of a systematic review of both nearly 300 systems of records and many hundreds of information technology systems that were either part of legacy agencies or incorporated into new components. Since starting with two people, the Chief Privacy Officer and an administrative assistant, the Privacy Office has grown in size and, through investments in personnel and hard work, created a comprehensive process to serve the long-term interests of DHS by providing the most complete and thorough privacy office possible.

Accomplishment 1: The Privacy Office has made significant progress in reviewing and approving PIAs but faces an increasing workload.

Response:

The Privacy Office appreciates GAO's acknowledgment of its success in creating a standardized process for developing privacy compliance documentation for individual systems and for managing the overall compliance process. The Department's robust compliance framework for PIAs and SORNs enables programs to effectively articulate the manner in which DHS uses personally identifiable information and informs the public of how the Department ensures that those uses of information are privacy protective.

www.dhs.gov

Accomplishment 2: The Privacy Office has taken steps to integrate privacy into DHS decision-making.

Response:

The Privacy Office appreciates the recognition of DHS's Data Privacy and Integrity Advisory Committee and the Privacy Office's ongoing series of public meetings and public workshops, both of which offer a public forum to discuss the complex issues raised by the use of personally identifiable information in the context of homeland security.

To assist the Privacy Office in embedding privacy into the very fabric of DHS program planning and design, the Privacy Office is extending its library of written guidance with a new guidance document focused on system development needs, which is entitled the Privacy Technology Implementation Guide (PTIG). The PTIG details the full range of privacy protection requirements, organized into a format that system developers and managers can use in practice. When completed, the PTIG will provide a structured resource to front-end the requirements of the privacy compliance process and further assist in thoroughly integrating privacy protections into the system development and operating process of DHS.

The Privacy Office also wishes to supplement the GAO's reference to the important international duties of the Privacy Office. In addition to reporting on the Undertakings associated with Passenger Name Records (PNR) and advising on the negotiations for the interim PNR agreement, as mentioned in the draft GAO report, the Privacy Office devotes significant efforts to outreach and negotiations in other international arenas. This is especially true with the European Union (EU), where the Privacy Office seeks to support DHS's critical mission to ensure the continued flow of traveler information for prescreening purposes, while at the same time bridge the differences between the U.S. and EU frameworks for respecting privacy. In just the last several months, the international policy team of the Privacy Office supported DHS's senior leadership at three U.S.-EU Justice and Home Affairs Ministerial meetings as well as numerous video conferences with our EU counterparts. The Privacy Office also continues to represent DHS privacy interests at regional privacy groups such as the Organization for Economic Cooperation and Development (OECD) and the Asian Pacific Economic Cooperation forum (APEC). The Privacy Office's efforts help shape the future standards for government to government sharing of personally identifiable information for legitimate homeland security purposes and ensure that such interactions sustain and do not erode privacy interests.

Since the completion of GAO's review, the Privacy Office issued its first Policy Guidance Memorandum regarding *The Collection, Use, Retention, and Dissemination of*

Information on Non-U.S. Persons (January 19, 2007).[1] This "Mixed System" memorandum standardizes and harmonizes existing practice and policy and is intended to support DHS's international policies as well as support responsibilities under the E-Government Act of 2002. The Mixed System memorandum is the first of what will be a series of memoranda providing privacy policy guidance to DHS leadership and components in support of the Privacy Office's main statutory duty to serve as the Secretary's primary policy maker on critical privacy issues.

Furthermore, the Privacy Office wishes to direct attention to its website (www.dhs.gov/privacy), which offers a substantial wealth of information about the Privacy Office and DHS's programs that use personally identifiable information. The website offers transcripts and indices to the materials of the meetings of the DHS Data Privacy and Integrity Advisory Committee, the privacy workshops, the Privacy Office reports, international activities of the Privacy Office, and the Privacy Impact Assessments approved by the Privacy Office. In addition to these materials, the Privacy Office published on its website the record of its Privacy Impact Assessment training session so that anyone interested in learning about PIAs and the PIA development process can benefit from the Privacy Office's efforts.

Recommendation 1: Designate full-time privacy officers at key DHS components, such as Customs and Border Patrol, the U.S. Coast Guard, Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

Response: Take under advisement

This recommendation is consistent with the DHS Privacy Act Compliance Management Directive (MD) No. 0470.2. Specifically, section V.B.1. of the MD directs Under Secretaries and all DHS Designated Officials to:

> *Appoint an individual with day-to-day responsibility for implementing the privacy provisions of the Privacy Act, and any other applicable statutory privacy requirement.*

The Privacy Office agrees that privacy officers play an important role at the component level. The privacy officers at the Transportation Security Administration and at the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) contribute significantly to success of the mission of the Privacy Office. While the GAO report notes that components with a designated officer have produced the majority of PIAs as a percentage of the total issued to date, this is just one example of the important contribution these component privacy officers make in embedding privacy into departmental programs. These component privacy officers provide day-to-day privacy expertise within their components to programs at all stages of development, ensuring that

[1] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

privacy is considered from the design through the implementation phase of every program within their component.

Recommendation 2: Implement a department-wide process for the biennial review of system-of-records notices, as required by OMB.

Response: Concur.

The Privacy Office developed the Privacy Threshold Analysis (PTA) in order to understand which systems at DHS handle or involve personally identifiable information and, of those systems, which need Privacy Impact Assessments (PIA) and, based on the analysis of the PIA, identify which systems need new or updated System of Records Notices (SORN). The Privacy Office found that the most expedient process to ensure overall privacy compliance focuses on the development of the PIA and then begins work on the corresponding SORN, because the PIA helps identify the appropriate purposes, routine uses for disseminating information, types of information, categories of individuals affected, and, if applicable and appropriate, exemptions from certain Privacy Act requirements for the system of records.

The Privacy Office developed a two prong approach to reviewing the legacy SORNs and updating them appropriately. As noted in the GAO draft report, the Privacy Office has a well-developed PIA compliance process. Part of that process identifies the legacy SORNs and determines whether an updated or new SORN must be published. Next, the component, the Privacy Office, and the DHS Office of General Counsel review the SORN to issue a DHS SORN that is updated appropriately to describe the program as it exists under DHS and its homeland security mission. Programs making operational enhancements may not implement any updates until DHS publishes the SORN in the *Federal Register* and the Privacy Office approves the PIA.

In the second prong of the SORN review, the Privacy Office is systematically reviewing by component the legacy SORNs and in order to issue updated SORNs on a schedule that prioritizes those systems with the most sensitive personally identifiable information.

As of April 2007, the Privacy Office identified 260 SORNs of which 211 are legacy SORNs. By the end of FY2007, the Privacy Office will issue an updated System of Records Notice Guide to help in the drafting process. The Privacy Office is also developing a library of acceptable routine uses that components can use to identify appropriate routine uses as they review and develop their own SORNs. This will likely reduce the time needed to review draft SORNs.

This two pronged approach will permit the Privacy Office to work with DHS components to evaluate methodically, and in a timely fashion, all of the existing SORNs to determine if the need exists to re-issue, remove, or re-draft each notice. The Privacy Office has met with a number of components and will meet with all others to establish appropriate timelines to accomplish this goal consistent with the Privacy Offices responsibilities under issued OMB guidance.

Recommendation 3: Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report development including departmental clearance.

Response: Concur.

The Privacy Office fully acknowledges the need for the timely issuance of its reports, including its annual report, and applies full effort to meet any report deadlines. The Privacy Office will work those components and programs impacted by its reports to provide for both full collaboration and coordination within DHS and timely issuance of its reports.

Recommendation 4: Ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

Response: Concur.

While the Privacy Office acknowledges that Section 222 of the Homeland Security Act of 2002 requires the Privacy Office to include in its annual report to Congress a number of items of information, including "complaints of privacy violations," the Privacy Office interprets this list as descriptive, rather than prescriptive, in terms of where this information appears in the report. As such, the last report noted the privacy complaints the Privacy Office received within the substantive discussion of the actions of the Privacy Office.

For example, in the section discussing the reports provided to Congress, the last annual report notes the *Report on the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties* and the *Data Mining Report*. Although both reports were completed in response to Congressional requests, they dealt with privacy issues that surrounded complaints received by the Department. Additionally, this annual report discussed the work on the *Secure Flight* and *MATRIX* reports, which have since been issued and were directly responsive to complaints received by the Privacy Office. Further, the annual report noted the work of the Privacy Office with regard to the Undertakings concerning Passenger Name Records and REAL ID, issues that had generated a number of comments to the Privacy Office from privacy groups, if not specifically privacy complaints. Thus, throughout the last annual report, the Privacy Office noted issues of interest brought to its attention regarding privacy and DHS.

Nonetheless, the Privacy Office agrees that for the sake of reporting clarity that a consolidated reporting structure for privacy complaints within the annual report would assist in assuring Congress and the public that the Privacy Office is addressing the complaints that it receives.

The Department thanks you for the work that was done on this engagement and the cooperation received from the GAO team.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Linda D. Koontz, (202) 512-6420, koontzl@gao.gov

Staff Acknowledgments

Major contributors to this report were John de Ferrari, Assistant Director; Nancy Glover; Anthony Molet; David Plocher; and Jamie Pressman.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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

PRINTED ON RECYCLED PAPER