United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EDT
Tuesday, July 24, 2007

HOMELAND SECURITY

DHS Privacy Office Has Made Progress but Faces Continuing Challenges

Statement of Linda Koontz
Director, Information Management Issues

July 2007

HOMELAND SECURITY

DHS Privacy Office Has Made Progress but Faces Continuing Challenges

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-1024T, a testimony before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

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 and ensuring compliance with the Privacy Act of 1974, and (3) preparing and issuing annual reports and reports on key privacy concerns.

GAO was asked to testify on its recent report examining progress made by the DHS Privacy Office in carrying out its statutory responsibilities. GAO compared statutory requirements with Privacy Office processes, documents, and activities.

What GAO Recommends

In its report, GAO recommended 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 report and described actions initiated to address GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1024T.

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

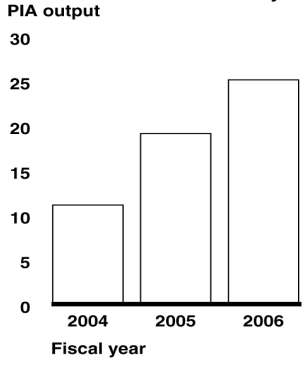
What GAO Found

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 established 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 systems requiring such assessments. 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 one aspect of ensuring compliance with the Privacy Act—updating public notices 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.

Madam Chairwoman and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss progress made and challenges faced by the Department of Homeland Security's (DHS) Privacy Office. 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 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]

As the federal government obtains and processes personal information[2] about its citizens and residents in increasingly diverse ways to better secure our homeland, it is important that this information be properly protected and the privacy rights of individuals respected. Advances in information technology make it easier than ever for DHS and other agencies to acquire data on individuals, analyze it for a variety of purposes, and share it with other governmental and nongovernmental entities. Further, the demands of the war on terror have led agencies to seek ways to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. It is in this context that the DHS Privacy Officer is charged with ensuring that the privacy rights of individuals remain adequately addressed.

Formally established with the appointment of the first Chief Privacy Officer in April, 2003, the DHS Privacy Office is responsible for ensuring that the department 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,

[1]Homeland Security Act of 2002, Sec. 222, Pub. L. No. 107-296 (Nov. 25, 2002).

[2]For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including *personally identifiable information*, which refers to any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

and the E-Government Act of 2002 (E-Gov Act).[3] The Privacy Office's major responsibilities can be summarized into four broad categories: (1) reviewing and approving privacy impact assessments (PIA) of the risks associated with information technology used to process personal information,[4] as required by the E-Government Act, (2) integrating privacy considerations into DHS decision making, (3) reviewing and approving public notices required by the Privacy Act, and (4) preparing and issuing reports.

My testimony today is based on a report that we recently issued.[5] In that report, we assessed progress made by the DHS Privacy Office in carrying out its responsibilities under federal privacy laws, including the Homeland Security Act and the E-Gov Act. In conducting work for that report, we compared statutory requirements with Privacy Office processes, documents, and activities. Our work was performed in accordance with generally accepted government auditing standards.

Today, after a brief summary and a discussion of the establishment of the DHS Privacy Office and its major responsibilities, my remarks will focus on the results of our review of the DHS Privacy Office.

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

[3]Section 222 of the Homeland Security Act, as amended by section 8305 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 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. No. 107-347 (Dec. 17, 2002).

[4]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.

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

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, conducting 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 that 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 had reviewed, approved, and issued 56 new and revised Privacy Act public notices as of February 2007, 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. 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 made 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 to issue reports in a timely manner. 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. The Chief Privacy Officer 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.[6] 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. In addition, 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.

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. As of February 2007, the Privacy Office also had 9 full-time and 3 half-time contractor staff. 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.

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

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 these four broad categories:

1. reviewing and approving PIAs,
2. integrating privacy considerations into DHS decision making,
3. reviewing and approving public notices required by the Privacy Act, and
4. preparing and issuing reports.

Reviewing and approving PIAs

The Privacy Office is responsible for ensuring departmental compliance with the privacy provisions of the E-Gov Act. Specifically, 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. 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.

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

[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).

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.

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 notice. This notice must include information such as the type of

[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. No. 107-347 (Dec. 17, 2002).

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

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.[11] The Intelligence Reform and Terrorism Prevention Act of 2004 also required the Chief Privacy Officer to submit a report to Congress on the impact on privacy and civil liberties 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 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.

[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).

[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) and (k).

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

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 PIAs to ensure departmental compliance with the privacy provisions (section 208) of the E-Gov Act of 2002. The Privacy Office has established a PIA compliance framework to carry out this responsibility. 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,[12] the Privacy Office's guidance goes further in several areas. For example, the guidance does not exempt national security systems[13] 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 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 radio frequency identification (RFID).

The Privacy Office has taken steps to continually improve its PIA guidance. Initially released in February 2004, the guidance has been updated each year since then. 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 information collection, the latest guidance requires program officials to explain how the collection supports the purpose(s) of the system or program and the mission of the organization. The guidance also reminds agencies that the information collected should be relevant and necessary to accomplish the stated purpose(s) and mission. To accompany its written guidance, the Privacy Office has also developed a PIA template and conducted a number of training sessions to further assist DHS personnel.

Our analysis of published DHS PIAs shows significant quality improvements in those completed recently compared with those from 2 or

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

[13]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.

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 assessments of 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. Earlier PIAs did 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.

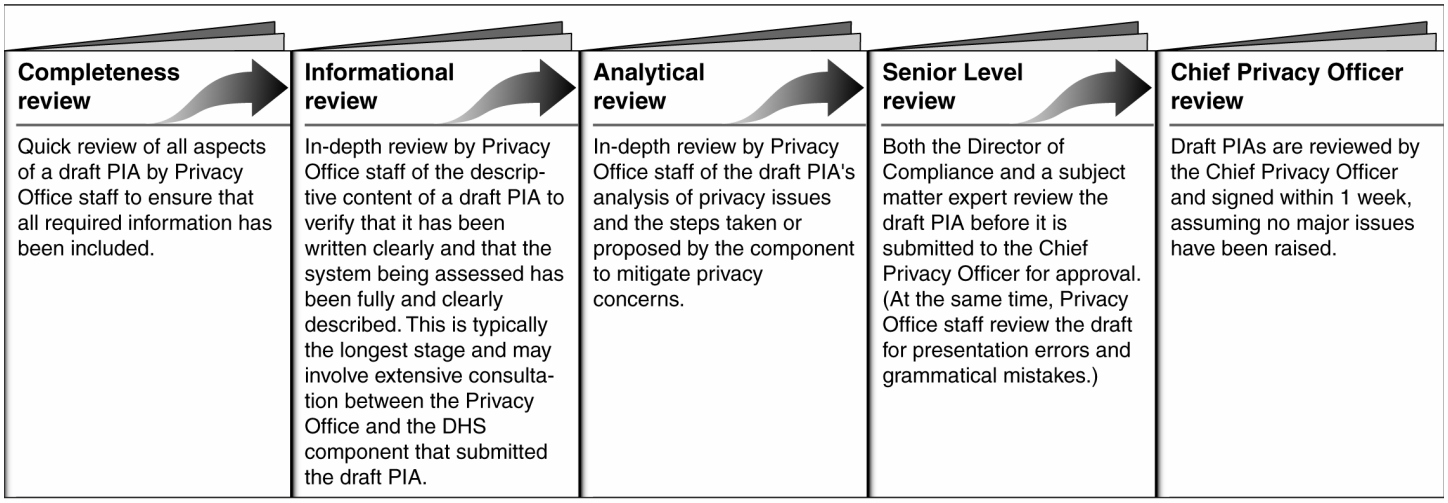
In addition to written guidance, the Privacy Office has also taken steps to integrate PIA development into the department's established operational processes. For example, the Privacy Office is using the OMB Exhibit 300 budget process[14] as an opportunity to ensure that systems containing personal information 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 privacy considerations during systems development, as envisioned by OMB's guidance.

Because of concerns expressed by component officials that the Privacy Office's review process takes a long time and is difficult to understand, the office has made efforts to improve the process and make it more transparent to DHS components. Specifically, the office has 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

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

review process is intended to take 5 to 6 weeks, with each stage intended to take 1 week. Figure 1 illustrates the stages of the review process.

Figure 1: 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.[15] Since 2004, PIA output by the Privacy Office has more than doubled. According to Privacy Office officials, the increase 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.

Because the Privacy Office has focused departmental attention on the development and review process and established a structured framework

[15]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 for 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."

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[16] 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.

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.

For example, in 2004, the first Chief Privacy Officer established the DHS Data Privacy and Integrity Advisory Committee to advise her and the

[16]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.

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. 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. According to Privacy Office officials, the additional instructions on the use of commercial data contained in the May 2007 PIA guidance update were based, in part, on the advisory committee's report on commercial data.

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

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. In June 2006, a workshop was held on the policy, legal, and operational frameworks for PIAs and privacy threshold analyses and

[17]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.

included a tutorial for conducting PIAs.[18] 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. In May 2004, an international agreement on the processing of this information was signed by DHS and the European Union.[19] Prior to the agreement, CBP established a set of terms for acquiring and protecting data on European Union citizens, referred to as the "Undertakings".[20] 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.

[18]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.

[19]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.

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

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.[21] 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.

REAL ID Act of 2005

Among other things, the REAL ID Act[22] requires DHS to consult with the Department of Transportation and the states in issuing 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

[21]71 *Federal Register* 60928-60932 (Oct. 17, 2006).

[22]Division B, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13 (May 11, 2005).

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.[23] 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.[24] 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.[25] Accordingly, we recommended that DHS, as well as other agencies, develop such 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

[23]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.

[24]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.

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

concerns will be fully addressed. For example, our previous work has highlighted problems in implementing privacy protections in specific DHS programs, including Secure Flight[26] and the ADVISE program.[27] 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. 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.

[26]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).

[27]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.[28]

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.

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

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

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.[29]

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.[30] 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.

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.

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

[30]These 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.

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 legal requirements, 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 statutory 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[31] 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 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.

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 Multi-state Anti-Terrorism Information Exchange 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.

[31]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.

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.[32] 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 or DHS officials who are outside the Privacy Office.[33] Until its reports are issued in a timely fashion, questions about the credibility and authority of the Privacy Office will likely remain.

[32]Section 522, Department of Homeland Security Appropriations Act, 2007 (Pub. L. No. 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."

[33]The Privacy Officer with Enhanced Rights Act was introduced as Subtitle B of Title VIII of H.R. 1, "Implementing the 9/11 Commission Recommendations Act of 2007," introduced on January 5, 2007. This bill would also grant the Privacy Officer investigative authority, including subpoena power.

Implementation of GAO Recommendations Would Lead to Improvements in Privacy Office Operations

In order to ensure that Privacy Act notices reflect current DHS activities and to help the Privacy Office meet its obligations and issue reports in a timely manner, in our report we recommended that the Secretary of Homeland Security take the following four actions:

1. 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.

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

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.

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

Concerning our recommendation that it designate full-time privacy officers in key departmental components, DHS noted in comments on a draft of our report 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." However, according to Privacy Office officials, as of July 2007, no such designations have been made. Until DHS appoints such officers, the Privacy Office will not benefit from their potential to help speed the processing of PIAs, nor will component programs be in a position to benefit from the privacy expertise these officials could provide.

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. As of July 2007, DHS officials reported that they have 215 legacy SORNs that need to be reviewed and either revised or retired. Until DHS reviews and updates all of its legacy notices as required by federal guidance, it

cannot assure the public that its notices reflect current uses and protections of personal information.

Concerning our recommendations 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.

In summary, 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. The office faces continuing challenges in reducing its backlog of systems requiring PIAs, ensuring that system-of-records notices are kept up to date, and in issuing reports in a timely fashion.

Mr. Chairman, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

Contacts and Acknowledgments

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions include John de Ferrari, Nancy Glover, Anthony Molet, David Plocher, and Jamie Pressman.

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'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