United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, March 21, 2007

HOMELAND SECURITY

Continuing Attention to Privacy Concerns is Needed as Programs Are Developed

Statement of Linda D. Koontz
Director, Information Management Issues

March 21, 2007

HOMELAND SECURITY

Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-630T, a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

Why GAO Did This Study

Advances in information technology make it easier than ever for the Department of Homeland Security (DHS) and other agencies to obtain and process information about citizens and residents in many ways and for many purposes. The demands of the war on terror also drive agencies to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. Recognizing that securing the homeland and protecting the privacy rights of individuals are both important goals, the Congress has asked GAO to perform several reviews of DHS programs and their privacy implications over the past several years.

For this hearing, GAO was asked to testify on key privacy challenges facing DHS. To address this issue, GAO identified and summarized issues raised in its previous reports on privacy and assessed recent governmentwide privacy guidance.

What GAO Recommends

Because GAO has already made privacy-related recommendations in its earlier reports, it is making no further recommendations at this time. Officials have taken action or have said they are in the process of taking action to address the recommendations. Implementation is critical to ensuring that privacy protections are in place throughout key DHS programs and activities.

www.gao.gov/cgi-bin/getrpt?GAO-07-630T.

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

As it develops and participates in important homeland security activities, DHS faces challenges in ensuring that privacy concerns are addressed early, are reassessed when key programmatic changes are made, and are thoroughly reflected in guidance on emerging technologies and uses of personal data. GAO's reviews of DHS programs have identified cases where these challenges were not fully met. For example, increased use by federal agencies of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—has been accompanied by uncertainty regarding privacy requirements and oversight of such systems. As described in a recent GAO report, DHS did not assess privacy risks in developing a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), as required by the E-Government Act of 2002. ADVISE is a data mining tool under development intended to help the department analyze large amounts of information. Because privacy had not been assessed and mitigating controls had not been implemented, DHS faced the risk that uses of ADVISE in systems containing personal information could require costly and potentially duplicative retrofitting at a later date to add the needed controls.

GAO has also reported on privacy challenges experienced by DHS in reassessing privacy risks when key programmatic changes were made during development of a prescreening program for airline passengers. The Transportation Security Administration (TSA) has been working to develop a computer-assisted passenger prescreening system, known as Secure Flight, to be used to evaluate passengers before they board an aircraft on domestic flights. GAO reported that TSA had not fully disclosed uses of personal information during testing of Secure Flight, as required by the Privacy Act of 1974. To prevent such problems from recurring, TSA officials recently said that they have added privacy experts to Secure Flight's development teams to address privacy considerations on a continuous basis as they arise.

Another challenge DHS faces is ensuring that privacy considerations are addressed in the emerging information sharing environment. The Intelligence Reform and Terrorism Prevention Act of 2004 requires the establishment of an environment to facilitate the sharing of terrorism information, as well as the issuance of privacy guidelines for operation in this environment. Recently issued privacy guidelines developed by the Office of the Director of National Intelligence provide only a high-level framework for privacy protection. While DHS is only one participant, it has the responsibility to ensure that the information under its control is shared with other organizations in ways that adequately protect privacy. Accordingly, it will be important for the department to clearly establish departmental guidelines so that privacy protections are implemented properly and consistently.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss issues in enhancing personal privacy while meeting homeland security needs. As the federal government obtains and processes personal information[1] about 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 the Department of Homeland Security (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 drive agencies to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. Given that securing the homeland and protecting the privacy rights of individuals are both important goals, it is incumbent on the government to find ways to do both well without compromising either.

As requested, my statement will focus on key privacy challenges facing DHS as it develops systems and methods for fighting the war on terror. After a brief description of the laws and guidance that apply to federal agency use of personal information, I will summarize our work on key programs and activities in which privacy considerations have been prominent, including data mining, passenger prescreening, use of commercial data, and radio frequency identification technology. I will also comment on the department's role in participating in the governmentwide information sharing environment, which is being established by the

[1]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.

administration to facilitate the sharing of terrorism information among governmental entities.[2]

To address key privacy challenges facing DHS, we identified and summarized issues raised in our previous reports on privacy, including our work on data mining,[3] passenger prescreening,[4] commercial data,[5] and radio frequency identification applications.[6] We also assessed recent governmentwide privacy guidance for the information sharing environment and identified privacy challenges DHS is likely to face as a participant. We conducted our work in accordance with generally accepted government auditing standards. To provide additional information on our previous privacy-related work, I have included, as attachment 1, a list of pertinent GAO publications.

Results in Brief

As it develops and participates in important homeland security activities, DHS faces challenges in ensuring that privacy concerns are addressed early, are reassessed when key programmatic

[2]For more information, see GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[3]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) and *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, GAO-05-866 (Washington, D.C.: Aug. 15, 2005).

[4]GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T (Washington, D.C.: Feb. 13, 2007) and *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).

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

[6]GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005) and *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248 (Washington, D.C.: Dec. 6, 2006).

changes are made, and are thoroughly reflected in guidance on emerging technologies and uses of personal data. Our reviews of DHS programs have identified cases where these challenges were not fully met. For example:

- *Ensuring that data mining efforts do not compromise privacy protections*. Increased use by federal agencies of data mining—the analysis of large amounts of data to uncover hidden patterns and relationships—has been accompanied by uncertainty regarding privacy requirements and oversight of such systems. For example, as described in our recent report,[7] DHS did not assess privacy risks in developing a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), as required by the E-Government Act of 2002. Because privacy had not been assessed and mitigating controls had not been implemented, DHS faced the risk that ADVISE-based systems containing personal information could require costly and potentially duplicative retrofitting at a later date to add the needed controls. Accordingly, we recommended that DHS immediately conduct a privacy impact assessment of the ADVISE tool to identify privacy risks and implement privacy controls to mitigate those risks. In its comments DHS stated that it is currently developing a "Privacy Technology Implementation Guide" to be used to conduct a PIA.
- *Ensuring privacy protection in developing and implementing prescreening programs for airline passengers*. In accordance with a requirement set forth in the Aviation and Transportation Security Act, the Transportation Security Administration (TSA) has been working to develop a computer-assisted passenger prescreening system, known as Secure Flight, to be used to evaluate passengers before they board an aircraft domestically. In previous work, we reported that TSA had not fully disclosed uses of personal information during testing of Secure Flight, as required by the Privacy Act of 1974. To prevent such problems from recurring, TSA officials recently said that they have added privacy experts to Secure Flight's development teams to address privacy considerations on a continuous basis as they arise.

[7] GAO-07-293.

- *Controlling the collection and use of personal information obtained from commercial sources, known as "information resellers."* A major task confronting federal agencies, especially those engaged in antiterrorism tasks, is to ensure that information obtained from resellers is being appropriately used and protected. In previous work, we reported that agencies were uncertain about the applicability of privacy requirements to this information, which led to inconsistencies in how it was treated. For example, public notices required by the Privacy Act did not always disclose the use of information from resellers. We recommended that DHS develop a policy concerning the use of such information, which according to the DHS Privacy Office is currently in draft.
- *Ensuring that applications using radio frequency identification technology (RFID) protect privacy consistently.* RFID technology uses wireless communication to transmit data and thus electronically identify, track, and store information on tags attached to or embedded in objects. Our recent work on US-VISIT[8]—a DHS program to collect data on selected foreign nationals entering and exiting the United States—identified problems with the use of RFID for human identification.[9] Although the Secretary of Homeland Security has announced that RFID use by US-VISIT is to be discontinued, another DHS border control program, the Western Hemisphere Travel Initiative, still plans to use the technology. Without departmental guidance on the use of RFID, DHS programs may use the technology inconsistently, potentially creating unnecessary privacy risks. According to the DHS Privacy Office, it is considering developing guidance to address the use of specific technologies, including RFID.
- *Ensuring that privacy considerations are addressed consistently and effectively in the information sharing environment.* As directed by the Intelligence Reform and Terrorism Prevention Act of 2004, the administration has taken steps, beginning in 2005, to establish an information sharing environment to facilitate the sharing of terrorism information. However, privacy guidelines recently issued for the information sharing environment provide

[8]US-VISIT is an abbreviation for United States Visitor and Immigrant Status Indicator Technology.

[9]GAO-07-248.

only a high-level framework for ensuring privacy protection and do not address how the collection of information is to be limited. Because DHS participates in the information sharing environment, potentially sharing information with many other intelligence and law enforcement entities both within and outside the federal government, it will be important for the department to ensure that departmental guidelines are clearly established so that privacy protections are implemented properly and consistently.

We have made recommendations to DHS in several of these areas to ensure that privacy issues are adequately addressed, and officials have taken action or told us they are in the process of taking action to address them. Implementation of these recommendations is critical to ensuring that privacy protections are in place throughout key DHS programs and activities.

Background: Federal Laws and Guidance Govern Use of Personal Information in Federal Agencies

The major requirements for the protection of personal privacy by federal agencies are specified in two laws, the Privacy Act of 1974 and the E-Government Act of 2002. The Federal Information Security Management Act of 2002 (FISMA) also addresses the protection of personal information in the context of securing federal agency information and information systems.

The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a "system-of-records notice": that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals

about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.[10] Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes. For example, the act requires that to the greatest extent practicable, personal information should be collected directly from the subject individual when it may affect an individual's rights or benefits under a federal program.

The provisions of the Privacy Act are largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices, which were first proposed in 1973 by a U.S. government advisory committee;[11] these principles were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. Since that time, the Fair Information Practices have been widely adopted as a standard benchmark for evaluating the adequacy of privacy protections. Attachment 2 contains a summary of the widely used version of the Fair Information Practices adopted by the Organization for Economic Cooperation and Development in 1980.

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems and information collections by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to Office of Management and Budget (OMB) guidance,[12] a PIA is to (1) ensure that handling

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

[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* (Washington, D.C.: July 1973).

[12]Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003). OMB is tasked with providing guidance to agencies on how to implement the provisions of the E-Government Act, the Privacy Act, and FISMA.

conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form, or (2) before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available,[13] they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

FISMA also addresses the protection of personal information. It defines 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.[14] Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy.

To oversee its implementation of privacy protections, DHS has established a Chief Privacy Officer, as directed by the Homeland Security Act of 2002.[15] According to the act, the Chief Privacy Officer

[13]The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, by publication in the *Federal Register*, or by other means. Pub. L. 107-347, § 208(b)(1)(B)(iii).

[14]FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

[15]Pub. L. No. 107-296, § 222 (Nov. 25, 2002).

is responsible for, among other things, "assuring that the use of technologies sustain[s], and do[es] not erode privacy protections relating to the use, collection, and disclosure of personal information," and "assuring 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."

Privacy Considerations Need Continuing Attention As Programs and Systems Are Developed

As it develops and participates in important homeland security activities, DHS faces challenges in ensuring that privacy concerns are addressed early, are reassessed when key programmatic changes are made, and are thoroughly reflected in guidance on emerging technologies and uses of personal data. Our reviews of DHS programs have identified cases where these challenges were not fully met, including data mining, airline passenger prescreening, use of data from commercial sources, use of personal identification technologies (especially RFID), and development of an information sharing environment. I will now discuss each of these subjects in greater detail.

Ensuring that Data Mining Efforts Do Not Compromise Privacy Protections

Many concerns have been raised about the potential for data mining programs to compromise personal privacy. In our May 2004 report on federal data mining efforts, we defined data mining as the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.[16] As we noted in our report, mining government and private databases containing personal information raises a range of privacy concerns.

[16] GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548 (Washington, D.C.: May 4, 2004).

In the government, data mining was initially used to detect financial fraud and abuse. However, its use has greatly expanded. Among other purposes, data mining has been used increasingly as a tool to help detect terrorist threats through the collection and analysis of public and private sector data. Through data mining, agencies can quickly and efficiently obtain information on individuals or groups from large databases containing personal information aggregated from public and private records. Information can be developed about a specific individual or a group of individuals whose behavior or characteristics fit a specific pattern. For example, terrorists can be tracked through travel and immigration records, and potential terrorist-related activities, including money transfers and communications, can be pinpointed. The ease with which organizations can use automated systems to gather and analyze large amounts of previously isolated information raises concerns about the impact on personal privacy. As a July 2006 report by the DHS Privacy Office points out, "privacy and civil liberties issues potentially arise in every phase of the data mining process."[17] Potential privacy risks include improper access or disclosure of personal information, erroneous associations of individuals with undesirable activities, misidentification of individuals with similar names, and misuse of data that were collected for other purposes.

Our recent report notes that early attention to privacy in developing a data mining tool known as ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement) could reduce risks that personal information could be misused.[18] ADVISE is a data mining tool under development intended to help DHS analyze large amounts of information. It is designed to allow an analyst to search for patterns in data—such as relationships among people, organizations, and events—and to produce visual representations of these patterns, referred to as semantic graphs. The intended benefit of the ADVISE tool is to help detect threatening activities by facilitating the analysis of large amounts of data. Although the tool

[17]DHS, *Data Mining Report: DHS Privacy Office Response to House Report 108-774* (July 6, 2006), p. 12.

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

is being considered for several different applications within DHS, none of them are yet operational. DHS is currently in the process of testing the tool's effectiveness.

DHS did not conduct a PIA as it developed the ADVISE tool, as required by the E-Government Act of 2002. A PIA, if it had been completed, would identify specific privacy risks and help officials determine what controls were needed to mitigate those risks. DHS officials believed that ADVISE did not need to undergo such an assessment because the tool itself did not contain personal data. However, the intended uses of the tool included personal data, and the E-Government Act and related guidance emphasize the need to assess privacy risks early in system development. Further, if an assessment were conducted and privacy risks identified, a number of controls could be built into the tool to mitigate those risks. Because privacy had not been assessed and mitigating controls had not been implemented, the department faced the risk that systems based on ADVISE that also contained personal information could require costly and potentially duplicative retrofitting to add the needed controls. We made recommendations to DHS to conduct a PIA of the ADVISE tool and implement privacy controls, as needed, to mitigate any identified risks. In its comments, DHS stated that it is currently developing a "Privacy Technology Implementation Guide" to be used to conduct a PIA.

Broadly considered, data mining is a tool that has the potential to provide valuable assistance to analysts and investigators as they pursue the war on terror. However, it has been challenging for DHS to thoroughly consider and address privacy concerns early enough in its attempts to develop data mining tools and applications. As the department moves forward with ADVISE and other data mining activities, close attention to privacy will remain a critical concern.

Ensuring Privacy Protection in Developing and Implementing Prescreening Programs for Airline Passengers

An example of the importance of ongoing attention to privacy can be taken from TSA's development of passenger prescreening programs. TSA is responsible for securing all modes of transportation while facilitating commerce and the freedom of

movement for the traveling public. Passenger prescreening is one program among many that TSA uses to secure the domestic aviation sector. The process of prescreening passengers—that is, determining whether airline passengers might pose a security risk before they reach the passenger-screening checkpoint—is used to focus security efforts on those passengers that represent the greatest potential threat.

In accordance with a requirement set forth in the Aviation and Transportation Security Act, TSA has been working since 2003 to develop a computer-assisted passenger prescreening system to be used to evaluate passengers before they board an aircraft on domestic flights. An early version of that system, known as the Computer-Assisted Passenger Prescreening System II, was canceled in 2004 based in part on concerns about privacy and other issues expressed by us and others.[19] In its place, TSA announced a new passenger prescreening program, called Secure Flight, that would be narrower in scope and designed to avoid problems that had been raised about the previous program. Aspects of the new Secure Flight system underwent development and testing in 2005.

In July 2005, we reported on privacy problems associated with testing of Secure Flight.[20] In 2004, TSA had issued privacy notices in the *Federal Register* that included descriptions of how personal information drawn from commercial sources would be used during planned upcoming tests. However, these notices did not fully inform the public about the procedures that TSA and its contractors would follow for collecting, using, and storing commercial data. In addition, the scope of the data used during commercial data testing was not fully disclosed. Specifically, a contractor, acting on behalf of the agency, collected more than 100 million commercial data records containing personal information such as name, date of birth,

[19]See GAO, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004).

[20]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).

and telephone number without informing the public. As a result, the public did not receive the full protections of the Privacy Act. In its comments on our findings, DHS stated that it recognized the merits of the issues we raised, and that TSA had acted immediately to address them.

The privacy problems faced in developing Secure Flight arose not because it was prohibitively difficult to protect privacy while prescreening airline passengers, but because TSA had not reassessed privacy risks when key programmatic changes were made and taken appropriate steps to mitigate them. Recently, TSA officials stated that as they work to restructure the Secure Flight program, they plan a more privacy-enhanced program by addressing concerns identified by us and others. For example, officials stated that the program no longer plans to use commercial data. Officials also stated that they have added privacy experts to the system development teams to address privacy issues as they arise. It is encouraging that TSA is now including privacy experts within its development teams, with the express goal of continuously monitoring privacy concerns. We will continue to assess TSA's efforts to manage system privacy protections as part of our ongoing review of the program.

Controlling the Collection and Use of Personal Information Obtained from Information Resellers

A major task confronting federal agencies, especially those engaged in antiterrorism tasks, is to ensure that information obtained from resellers is being appropriately used and protected. In fiscal year 2005, DHS reported planning to spend about $9 million on acquiring personal information from information resellers.[21] The information was acquired chiefly for law enforcement purposes, such as developing leads on subjects in criminal investigations, and for detecting fraud in immigration benefit applications (part of enforcing the immigration laws). For example, the agency's largest

[21]Information resellers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers, which include both private-sector businesses and government agencies.

investigative component, U.S. Immigration and Customs Enforcement—the largest user of personal information from resellers—collects data such as address and vehicle information for criminal investigations and background security checks. DHS also reported using information resellers in its counterterrorism efforts. For example, as already discussed, TSA used data obtained from information resellers as part of a test associated with the development of Secure Flight.

In our report on the acquisition of personal information from resellers by agencies such as DHS, we noted that the agencies' practices for handling this information did not always reflect the Fair Information Practices.[22] For example, system-of-records notices issued by these agencies did not always state that agency systems could incorporate information from data resellers, a practice inconsistent with the principle that the purpose for a collection of personal data should be disclosed beforehand and its use limited to that purpose. Furthermore, accountability was not ensured, as the agencies did not generally monitor usage of personal information from resellers; instead, they relied on end users to be responsible for their own behavior. Contributing to the uneven application of the Fair Information Practices was a lack of agency policies, including at DHS, that specifically address these uses.

Reliance on information from resellers is an emerging use of personal data for which the government has been challenged to develop appropriate guidance. We recommended that DHS and other agencies develop specific policies, reflecting the Fair Information Practices, for the collection, maintenance, and use of personal information obtained from resellers. According to the DHS Privacy Office, while a policy governing the department's use of commercial data is being drafted, the document has not yet been issued. Until the department issues clear guidance on this use, it faces the risk that appropriate privacy protections may not be in place consistently across its programs and applications.

[22] GAO-06-421.

Ensuring that Applications Using RFID Technology Protect Privacy Consistently

RFID is an automated data-capture technology that can be used to electronically identify, track, and store information contained on a tag. The tag can be attached to or embedded in the object to be identified, such as a product, case, or pallet. RFID technology provides identification and tracking capabilities by using wireless communication to transmit data. In May 2005, we reported that major initiatives at federal agencies that use or propose to use the technology included physical access controls and tracking assets, documents, or materials.[23] For example, DHS was using RFID to track and identify assets, weapons, and baggage on flights. The Department of Defense was also using it to track shipments.

In our May 2005 report we identified several privacy issues related to both commercial and federal use of RFID technology. Among these privacy issues is the potential for the technology to be used inappropriately for tracking an individual's movements, habits, tastes, or predilections. Tracking is real-time or near-real-time surveillance in which a person's movements are followed through RFID scanning.) Public surveys have identified a distinct unease with the potential ability of the federal government to monitor individuals' movements and transactions.[24] Like tracking, profiling—the reconstruction of a person's movements or transactions over a specific period of time, usually to ascertain something about the individual's habits, tastes, or predilections—could also be undertaken through the use of RFID technology. Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual's privacy.

Concerns also have been raised that organizations could develop secondary uses for the information gleaned through RFID

[23]GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005).

[24]GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

technology; this has been referred to as mission or function "creep." The history of the Social Security number, for example, gives ample evidence of how an identifier developed for one specific use has become a mainstay of identification for many other purposes, governmental and nongovernmental.[25] Secondary uses of the Social Security number have been a matter not of technical controls but rather of changing policy and administrative priorities.[26]

DHS uses and has made plans to use RFID technology to track individuals in several border security programs. This has been met with concern from the DHS Data Privacy and Integrity Advisory Committee, which reiterated our concerns that employing the technology for human identification poses privacy risks, including notice problems and potential for secondary use. One program that planned to make use of RFID was the US-VISIT program, a multibillion dollar program that collects, maintains, and shares information on selected foreign nationals who enter and exit the United States at over 300 ports of entry around the country. The incorporation of RFID into the program arose from the agency's requirement for a less costly alternative to biometric verification of visitors exiting the country.

We recently testified that US-VISIT RFID tests revealed numerous performance and reliability problems.[27] For example, the readers placed to detect identifying tags failed to do so for a majority of the RFID tags.[28] Faced with these test results, the Secretary of Homeland Security recently stated that the agency would cancel the use of RFID for US-VISIT.

[25]GAO, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (Washington, D.C.: May 31, 2002).

[26]For information on the practices and tools to mitigate these privacy issues, see GAO-05-551, pp. 22–24.

[27]GAO, *Homeland Security: US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to be Addressed*, GAO-07-499T (Washington, D.C.: Feb. 16, 2007).

[28]A US-VISIT program official explained that for vehicles exiting during RFID testing, one could "reasonably expect" a read rate of 70 percent. However, as the program office reported, tests conducted at the Blaine-Pacific Highway border station showed readers correctly identifying 14 percent of the travelers' tags.

However, despite having rejected RFID for US-VISIT, the department has endorsed the technology for another border control initiative, the proposed PASSport (People Access Security Service) system identification card, which is part of the Western Hemisphere Travel Initiative. The RFID-enabled PASSport card would serve as an alternative to a traditional passport for use by U.S. citizens who cross the land borders and travel by sea between the United States, Canada, Mexico, the Caribbean, or Bermuda.[29]

The department's varying approaches to the use of RFID for human identification suggests the need for a departmentwide policy that fully addresses privacy concerns. Unless DHS issues comprehensive guidance to direct the development and implementation of new technologies such as RFID, it faces the risk that appropriate privacy protections may not be implemented consistently across its programs and applications. According to the DHS Privacy Office, it is considering developing guidance to address the use of specific technologies, including RFID.

Ensuring that Privacy Considerations are Addressed Consistently and Effectively in the Information Sharing Environment

The challenges that DHS faces in protecting privacy extend beyond the need to consider and address privacy issues while developing its own programs and systems. The department also interacts with many other intelligence and law enforcement entities, both within and outside the federal government, and potentially shares information with them all. As with its own programs and systems, it will be important for DHS to ensure that privacy has been thoroughly considered and guidelines clearly established as it participates in the emerging information sharing environment.

As directed by the Intelligence Reform and Terrorism Prevention Act of 2004,[30] the administration has taken steps, beginning in 2005, to establish an information sharing environment to facilitate the sharing of terrorism information. The direction to establish an

[29]71 *Federal Register* 60928–60932 (Oct. 17, 2006).

[30]Pub. L. No. 108-458 (Dec. 17, 2004).

information sharing environment was driven by the recognition that before the attacks of September 11, 2001, federal agencies had been unable to effectively share information about suspected terrorists and their activities. In addressing this problem, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) recommended that the sharing and uses of information be guided by a set of practical policy guidelines that would simultaneously empower and constrain officials, closely circumscribing what types of information they would be permitted to share as well as the types they would need to protect. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. Accordingly, since January 2005, we have designated information sharing for homeland security a high-risk area.[31]

In developing guidelines for the information sharing environment, there has been general agreement that privacy considerations must be addressed. The Intelligence Reform Act called for the issuance of guidelines to protect privacy and civil liberties in the development and use of the information sharing environment, and the President reiterated that requirement in an October 2005 directive to federal departments and agencies. Based on the President's directive, a committee within the Office of the Director of National Intelligence was established to develop such guidelines, and they were approved by the President in November 2006.[32] According to its annual report for 2004–2006, the DHS Privacy Office has played a role in developing these guidelines.[33]

[31]For more information, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: Jan. 2007), p. 47, and *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington D.C.: Mar. 17, 2006).

[32]Information Sharing Environment Program Management Office, *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (Nov. 22, 2006).

[33] DHS, *Privacy Office Annual Report to Congress July 2004–July 2006* (Washington, D.C.: July 2006).

However, the guidelines as issued provide only a high-level framework for addressing privacy protection and do not include all of the Fair Information Practices. The 9-page document includes statements of principles, such as "purpose specification," "data quality," "data security," and "accountability, enforcement, and audit" that align with certain elements of the Fair Information Practices, but it provides little or no guidance on how these principles are to be implemented and does not address another key practice—limiting the collection of personal information. For example, as the policy director of the Center for Democracy and Technology has pointed out, a number of principles mentioned in the guidelines do not include any specificity on how they should be carried out.[34] The guidelines call for agencies to "take appropriate steps" when merging information about an individual from two or more sources to ensure that the information is about the same individual, but they give no indication of what steps would be adequate to achieve this goal. For example, no guidance is provided on gauging the reliability of sources or determining the minimum amount of information needed to determine that different sources are referring to the same individual. Likewise, the guidelines direct agencies to implement adequate review and audit mechanisms to ensure compliance with the guidelines but, again, do not specify the nature of these mechanisms, which could include, for example, the use of electronic audit logs that cannot be changed by individuals. Finally, the guidelines also direct agencies to put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control. No further guidance is provided about the essential elements of a complaint process or what sort of remedies to provide.

According to the DHS Privacy Office, individual agencies, including DHS, are to develop specific guidelines that implement the high-level framework embodied in the governmentwide guidelines. However, no overall DHS guidance on the protection of privacy within the context of the information sharing environment has yet

[34]James X. Dempsey, *Statement on behalf of the Markle Foundation Task Force on National Security in the Information Age before the President's Privacy and Civil Liberties Oversight Board* (Washington, D.C.: Dec. 5, 2006).

been developed. According to the Privacy Office, an effort is currently being initiated to develop such guidance.

While DHS is only one participant in the governmentwide information sharing environment, it has the responsibility to ensure that the information under its control is shared with other organizations in ways that adequately protect privacy. Until it adopts specific implementation guidelines, the department will face the risk that its information sharing activities may not protect privacy adequately.

In summary, DHS faces continuing challenges in ensuring that privacy concerns are addressed early, are reassessed when key programmatic changes are made, and are thoroughly reflected in guidance on emerging technologies and uses of personal data. We have made recommendations previously regarding ADVISE, Secure Flight, and use of information resellers, and officials have taken action or told us they are taking action to address our recommendations. Implementation of these recommendations is critical to ensuring that privacy protections are in place throughout key DHS programs and activities. Likewise, issuing guidance for participation in the information sharing environment will also be critical to ensure implementation of consistent, appropriate protections across the department.

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 Acknowledgements

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 Barbara Collier, Susan Czachor, John de Ferrari, Timothy Eagle, David Plocher, and Jamie Pressman.

Attachment I: Selected GAO Products Related to Privacy Issues

Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks. GAO-07-293. Washington, D.C.: February 28, 2007.

Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains. GAO-07-448T. Washington, D.C.: February 13, 2007.

Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry. GAO-07-248. Washington, D.C.: December 6, 2006.

Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data. GAO-06-674. Washington, D.C.: June 26, 2006.

Veterans Affairs: Leadership Needed to Address Information Security Weaknesses and Privacy Issues. GAO-06-866T. Washington, D.C.: June 14, 2006.

Privacy: Preventing and Responding to Improper Disclosures of Personal Information. GAO-06-833T. Washington, D.C.: June 8, 2006.

Privacy: Key Challenges Facing Federal Agencies. GAO-06-777T. Washington, D.C.: May 17, 2006.

Personal Information: Agencies and Resellers Vary in Providing Privacy Protections. GAO-06-609T. Washington, D.C.: April 4, 2006.

Personal Information: Agency and Reseller Adherence to Key Privacy Principles. GAO-06-421. Washington, D.C.: April 4, 2006.

Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information. GAO-06-385. Washington, D.C.: March 17, 2006.

Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain. GAO-05-866. Washington, D.C.: August 15, 2005.

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.

Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Under Way. GAO-05-710. Washington, D.C.: June 30, 2005.

Information Security: Radio Frequency Identification Technology in the Federal Government. GAO-05-551. Washington, D.C.: May 27, 2005.

Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed. GAO-05-356. Washington, D.C.: March 28, 2005.

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards. GAO-05-59. Washington, D.C.: November 9, 2004.

Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548. Washington, D.C.: May 4, 2004.

Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385. Washington, D.C.: February 12, 2004.

Privacy Act: OMB Leadership Needed to Improve Agency Compliance. GAO-03-304. Washington, D.C.: June 30, 2003.

Data Mining: Results and Challenges for Government Programs, Audits, and Investigations. GAO-03-591T. Washington, D.C.: March 25, 2003.

Technology Assessment: Using Biometrics for Border Security. GAO-03-174. Washington, D.C.: November 15, 2002.

Information Management: Selected Agencies' Handling of Personal Information. GAO-02-1058. Washington, D.C.: September 30, 2002.

Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766. Washington, D.C.: June 28, 2002.

Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards. GAO-02-352. Washington, D.C.: May 31, 2002.

Attachment 2: 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[35] and has been widely adopted.

Table 1: 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 upon 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.

[35] 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.

Principle	Description
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.

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