United States Government Accountability Office

GAO

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, July 31, 2012

PRIVACY

Federal Law Should Be Updated to Address Changing Technology Landscape

Statement of Gregory C. Wilshusen, Director
Information Security Issues

GAO-12-961T

July 31, 2012

PRIVACY

Federal Law Should Be Updated to Address Changing Technology Landscape

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-961T, a testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

The federal government collects and uses personal information on individuals in increasingly sophisticated ways, and its reliance on information technology (IT) to collect, store, and transmit this information has also grown. While this enables federal agencies to carry out many of the government's critical functions, concerns have been raised that the existing laws for protecting individuals' personal information may no longer be sufficient given current practices. Moreover, vulnerabilities arising from agencies' increased dependence on IT can result in the compromise of sensitive personal information, such as inappropriate use, modification, or disclosure.

GAO was asked to provide a statement describing (1) the impact of recent technology developments on existing laws for privacy protection in the federal government and (2) actions agencies can take to protect against and respond to breaches involving personal information. In preparing this statement, GAO relied on previous work in these areas as well as a review of more recent reports on security vulnerabilities.

What GAO Recommends

GAO previously suggested that Congress consider amending applicable privacy laws to address identified issues. GAO has also made numerous recommendations to agencies over the last several years to address weaknesses in policies and procedures related to privacy and to strengthen their information security programs.

View GAO-12-961T. For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Technological developments since the Privacy Act became law in 1974 have changed the way information is organized and shared among organizations and individuals. Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government. For example, GAO has reported on challenges in protecting the privacy of personal information relative to agencies' use of Web 2.0 and data-mining technologies.

While laws and guidance set minimum requirements for agencies, they may not protect personal information in all circumstances in which it is collected and used throughout the government and may not fully adhere to key privacy principles. GAO has identified issues in three major areas:

- **Applying privacy protections consistently to all federal collection and use of personal information.** The Privacy Act's protections only apply to personal information when it is considered part of a "system of records" as defined by the act. However, agencies routinely access such information in ways that may not fall under this definition.
- **Ensuring that use of personally identifiable information is limited to a stated purpose.** Current law and guidance impose only modest requirements for describing the purposes for collecting personal information and how it will be used. This could allow for unnecessarily broad ranges of uses of the information.
- **Establishing effective mechanisms for informing the public about privacy protections.** Agencies are required to provide notices in the *Federal Register* of information collected, categories of individuals about whom information is collected, and the intended use of the information, among other things. However, concerns have been raised whether this is an effective mechanism for informing the public.

The potential for data breaches at federal agencies also pose a serious risk to the privacy of individuals' personal information. OMB has specified actions agencies should take to prevent and respond to such breaches. In addition, GAO has previously reported that agencies can take steps that include

- assessing the privacy implications of a planned information system or data collection prior to implementation;
- ensuring the implementation of a robust information security program; and
- limiting the collection of personal information, the time it is retained, and who has access to it, as well as implementing encryption.

However, GAO and inspectors general have continued to report on vulnerabilities in security controls over agency systems and weaknesses in their information security programs, potentially resulting in the compromise of personal information. These risks are illustrated by recent security incidents involving individuals' personal information. Federal agencies reported 13,017 such incidents in 2010 and 15,560 in 2011, an increase of 19 percent.

Chairman Akaka, Ranking Member Johnson, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on the state of federal privacy and data security laws. These laws are intended to protect the privacy of Americans' personally identifiable information and specify measures that federal agencies can take to reduce the risk of breaches of sensitive personal information.

As you know, the increasingly sophisticated ways in which personal information is obtained and used by the federal government has the potential to assist in performing critical functions, such as helping to detect and prevent terrorist threats and enhancing online interactions with citizens. But these technological developments can also pose challenges in ensuring the protection of citizens' privacy. In addition, the increasing reliance by federal agencies on information technology (IT) has radically changed the way our government, our nation, and much of the world communicate and conduct business. While bringing significant benefits, this dependence on IT can also create vulnerabilities that can result in, among other things, the compromise of sensitive personal information through inappropriate use, modification, or disclosure.

In my testimony today, I will describe (1) the impact of recent technology developments on existing laws for privacy protection in the federal government, and (2) actions agencies can take to protect against and respond to breaches involving personal information. In preparing this statement in July 2012, we relied on our previous work in these areas. (Please see the related GAO products list at the end of this statement.) These products contain detailed overviews of the scope and methodology we used. We also reviewed more recent agency inspector general assessments of security vulnerabilities at federal agencies and information on security incidents from the U.S. Computer Emergency Readiness Team (US-CERT), media reports, and other publicly available sources. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agency collection or use of personal information is governed primarily by two laws: the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a record as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. The act defines a "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 through a system-of-records notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information.

Several provisions of the act require agencies to define and limit collection and use of personal information to predefined purposes. For example, it requires that, to the greatest extent practicable, personal information should be collected directly from the individual when it may affect that person's rights or benefits under a federal program. It also requires agencies to indicate whether the individual's disclosure of the information is mandatory or voluntary; the principal purposes for which the information is intended to be used; the routine uses that may be made of the information; and the effects on the individual, if any, of not providing the information. Further, in handling information they have collected, agencies are generally required to allow individuals to review their records, request a copy of their record, and request corrections to their information, among other things.

The E-Government Act of 2002 was passed, among other reasons, to enhance the protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). PIAs are analyses of how personal information is collected, stored, shared, and managed in a federal system.

Title III of the E-Government Act, known as the Federal Information Security Management Act of 2002 (FISMA),[1] established a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible for, among other things, providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. These protections are to provide federal information and systems with integrity—preventing improper modification or destruction of information, confidentiality—preserving authorized restrictions on access and disclosure, and availability—ensuring timely and reliable access to and use of information.

The privacy protections incorporated in the Privacy Act are based primarily on the Fair Information Practices—a set of widely recognized principles for protecting the privacy of personal information first developed by an advisory committee convened by the Secretary of Health, Education and Welfare in 1972 and revised by the Organization for Economic Cooperation and Development (OECD) in 1980. These practices underlie the major provisions of the Privacy Act and privacy laws and related policies in many countries, including Germany, Sweden, Australia, and New Zealand, as well as the European Union. They are also reflected in a variety of federal agency policy statements, beginning with an endorsement of the OECD principles by the Department of Commerce in 1981. The OECD version of the principles is shown in table 1.

[1]FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002), 44 U.S.C. § 3541, et seq.

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.
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: OECD.

The Privacy Act gives the Office of Management and Budget (OMB) responsibility for developing guidelines and providing assistance to and oversight of agencies' implementation of the act. OMB also has responsibility under the E-Government Act for developing PIA guidance and ensuring agency implementation of the PIA requirement. In July 1975, OMB issued guidance for implementing the provisions of the Privacy Act and has periodically issued additional guidance since then. OMB has also issued guidance on other data security and privacy-related issues including federal agency website privacy policies, interagency sharing of personal information, designation of senior staff responsible for privacy, data breach notification, and safeguarding personally identifiable information.

Technological Changes Have Made Key Elements of Privacy Laws Outdated

Technological developments since the Privacy Act became law in 1974 have radically changed the way information is organized and shared among organizations and individuals. Such advances have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government.

For example, we reported in 2010 on privacy challenges associated with agencies using Web 2.0 technologies, such as web logs ("blogs"), social networking websites, video- and multimedia-sharing sites, and "wikis."[2] While the Privacy Act clearly applies to personal information maintained in systems owned and operated by the federal government, agencies often take advantage of commercial Web 2.0 offerings, in which case they have less control over the systems that maintain and exchange information, raising questions about whether personal information contained in those systems is protected under the act.

While OMB subsequently issued guidance to federal agencies for protecting privacy when using web-based technologies,[3] we reported in June 2011 that agencies had made mixed progress in updating privacy policies and assessing privacy risks associated with their use of social media services, as required by OMB's guidance. A number of agencies had not updated their privacy policies or conducted PIAs relative to their use of third-party services such as Facebook and Twitter.[4] Accordingly, we recommended that 8 agencies update their privacy policies and that 10 agencies conduct required PIAs. Most of the agencies agreed with our recommendations; however, 5 have not yet provided evidence that they have updated their privacy policies and 4 have not yet provided documentation that they have conducted PIAs.

[2]GAO, *Information Management: Challenges In Federal Agencies' Use of Web 2.0 Technologies*, GAO-10-872T (Washington, D.C.: July 22, 2010).

[3]Office of Management and Budget, Memorandum M-10-23: *Guidance for Agency Use of Third-Party Websites and Applications* (Washington, D.C.: June 25, 2010).

[4]GAO, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605 (Washington, D.C.: June 28, 2011).

Another technology that has been increasingly used is data mining, which is used to discover information in massive databases, uncover hidden patterns, find subtle relationships in existing data, and predict future results. Data mining involves locating and retrieving information, including personally identifiable information, in complex ways.

In September 2011, we reported that the Department of Homeland Security (DHS) needed to improve executive oversight of systems supporting counterterrorism.[5] We noted that DHS and three of its component agencies—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and U.S. Citizenship and Immigration Services—had established policies that largely addressed the key elements and attributes needed to ensure that their data mining systems were effective and provided necessary privacy protections. However, we also noted, among other things, that DHS faced challenges in ensuring that all of its privacy-sensitive systems had timely and up-to-date PIAs. We recommended that that DHS develop requirements for providing additional scrutiny of privacy protections for sensitive information systems that are not transparent to the public through PIAs and investigate whether the information-sharing component of a certain data-mining system, the U.S. Immigration and Customs Enforcement Pattern Analysis and Information Collection program, should be deactivated until a PIA is approved that includes the component. DHS has taken action to address both of these recommendations.

Given the challenges in applying privacy laws and overseeing systems that contain personally identifiable information, the role of executives in federal departments and agencies charged with oversight of privacy issues is of critical importance. In 2008 we reported on agencies' designation of senior officials as focal points with overall responsibility for privacy.[6] Among other things, we were asked to describe the organizational structures used by agencies to address privacy requirements and assess whether senior officials had oversight over key functions. Although federal laws and OMB guidance require agencies to designate a senior official for privacy with privacy oversight responsibilities, we found that the 12 agencies we reviewed had varying organizational structures to address privacy responsibilities and that

[5]GAO, *Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism*, GAO-11-742 (Washington, D.C.: Sept. 7, 2011).

[6]GAO, *Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions,* GAO-08-603 (Washington, D.C.: May 30, 2008).

designated senior privacy officials did not always have oversight of all key privacy functions. Without such oversight, these officials may be unable to effectively serve as agency central focal points for information privacy. We recommended that six agencies take steps to ensure that their senior agency officials for privacy have oversight of all key privacy functions. Of the six agencies to which recommendations were made, four have provided evidence that they have fully addressed our recommendations.

Privacy Laws May Not Consistently Protect Personally Identifiable Information

In 2008, we issued a report on the sufficiency of privacy protections afforded by existing laws and guidance, in particular the Privacy Act, the E-Government Act, and related OMB guidance.[7] Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. We identified issues in three major areas:

Applying privacy protections consistently to all federal collection and use of personal information. The Privacy Act's definition of a system of records, which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, as may occur in data-mining systems, the act's protections do not apply. We previously reported that among the 25 agencies surveyed, the most frequently cited reason for collections of records not being considered Privacy Act systems of records was that the agency did not use a personal identifier to retrieve the information.[8] Factors such as these have led experts to agree that the Privacy Act's system-of-records construct is too narrowly defined. An alternative for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

Ensuring that use of personally identifiable information is limited to a stated purpose. According to the purpose specification and use limitation principles, the use of personal information should be limited to a

[7]GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

[8]GAO, *Privacy Act: OMB Leadership Needed to Improve Agency Compliance*, GAO-03-304 (Washington, D.C.: June 30, 2003).

specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. While purpose statements for certain law enforcement and antiterrorism systems might need to be phrased broadly enough so as not to reveal investigative techniques or the details of ongoing cases, very broadly defined purposes could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed. Examples for alternatives for addressing these issues include setting specific limits on the use of information within agencies and requiring agencies to establish formal agreements with external government entities before sharing personally identifiable information.

Establishing effective mechanisms for informing the public about privacy protections. According to the openness principle, the public should be informed about privacy policies and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection. Public notices are a primary means for establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Yet concerns have been raised that Privacy Act notices may not serve this function well. Although the *Federal Register* is the government's official vehicle for issuing public notices, an expert panel convened for GAO questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Among others, options for addressing concerns about public notices could include setting requirements to ensure that purpose, collection, and use limitations are better addressed in the content of privacy notices and revising the Privacy Act to require that all notices be published on a standard website.

Updating the Privacy Act Can Provide Benefits

Addressing these three areas could provide a number of benefits. First, ensuring that privacy protections are applied consistently to all federal collection and use of information could help ensure that information not retrieved by identifier (such as may occur in data-mining applications, for example) is protected in the same way as information retrieved by identifier. Further, limiting the use of personally identifiable information to a stated purpose could help ensure a proper balance between allowing government agencies to collect and use such information and limiting that collection and use to what is necessary and relevant. Lastly, a clear and

effective notice can provide individuals with critical information about what personal data are to be collected, how they are to be used, and the circumstances under which they may be shared. An effective notice can also provide individuals with information they need to determine whether to provide their personal information (if voluntary), or who to contact to correct any errors that could result in an adverse determination about them.

We noted that some of these issues—such as those dealing with limitations on use and mechanisms for informing the public—could be addressed by OMB through revisions of or supplements to existing guidance. However, we further stressed that unilateral action by OMB would not have the benefit of public deliberations regarding how best to strike an appropriate balance between the government's need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses.

Accordingly, we suggested that Congress consider amending applicable laws, such as the Privacy Act and E-Government Act, according to the alternatives we outlined, including

- revising the scope of the laws to cover all personally identifiable information collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

In commenting on a draft of our report, OMB officials noted that they shared our concerns about privacy and listed guidance that the agency has issued in the areas of privacy and information security. The officials stated that they believed it would be important for Congress to consider potential amendments to the Privacy and E-Government Acts in the broader contexts of other privacy statutes and that it would be important for Congress to evaluate fully the potential impact of revisions.

In addition, in October 2011, you, the Chairman, introduced a bill to amend the Privacy Act. This bill—The Privacy Act Modernization for the Information Age Act of 2011—would, among other things, revise the Privacy Act to cover all personally identifiable information collected, used, and maintained by the federal government and ensure that collection and use of personally identifiable information is limited to a stated purpose.

However, revisions to the Privacy and E-Government Acts have not yet been enacted.

Agencies Can Take Action to Mitigate the Risks of Data Breaches, But Such Breaches Have Continued to Proliferate

In addition to relevant privacy laws and federal guidance, a key component of protecting citizens' personal information is ensuring the security of agencies' information systems and the information they contain by, among other things, preventing data breaches and reporting those breaches when they occur. In 2006, in the wake of a security breach at the Department of Veterans Affairs resulting in the compromise of personal data on millions of U.S. veterans, we testified on preventing and responding to improper disclosures of personal information in the federal government.[9] We observed that agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are compromised. In particular, we noted two key steps agencies should take:

- Develop PIAs whenever information technology is used to process personal information. These assessments are a tool for agencies to fully consider the privacy implications of planned systems and data collections before implementation, when it may be easier to make critical adjustments.
- Ensure the implementation of a robust information security program as required by FISMA. Such a program includes periodic risk assessments; security awareness training; security policies, procedures, and practices, as well as tests of their effectiveness; and procedures for addressing deficiencies and for detecting, reporting, and responding to security incidents.

We also noted that data breaches could be prevented by limiting the collection of personal information, limiting the time such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on mobile devices.

OMB subsequently issued guidance that specifies minimum agency practices for using encryption to protect personally identifiable

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

information. Memorandums M-06-15, *Safeguarding Personally Identifiable information*, and M-06-16, *Protection of Sensitive Agency Information*, reiterated existing agency responsibilities to protect personally identifiable information, and directed agencies to encrypt data on mobile computers and devices and follow National Institute of Standards and Technology (NIST) security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter. In addition, OMB issued memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which restated the M-06-16 recommendations as requirements and also required the use of NIST-certified cryptographic modules for encrypting sensitive information

In 2008, we reported on the extent to which 24 major agencies had implemented encryption technologies.[10] We found that agencies' implementation of encryption and development of plans to implement encryption of sensitive information varied, and that from July through September 2007, the agencies collectively reported that they had not yet installed encryption technology on about 70 percent of their laptop computers and handheld devices. Accordingly, we made recommendations to selected agencies to strengthen practices for planning and implementing the use of encryption. The agencies generally agreed with the recommendations and we have assessed that 6 of the 18 recommendations have been addressed.

Despite preventive measures, data breaches can still occur, and when they do it is critical that proper response policies and procedures be in place. We testified in 2006[11] that notification to individuals affected by data breaches and/or the public has clear benefits, such as allowing people to take steps to protect themselves from identity theft. Such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection.

OMB issued guidance that updated and added requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information. Specifically, OMB memorandum M-06-19 directs agencies to report all incidents involving personally identifiable

[10]GAO, *Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains*, GAO-08-525 (Washington, D.C.: June 27, 2008).

[11]GAO-06-833T.

information to US-CERT within 1 hour of discovery of the incident. In addition, OMB memorandum M-07-16 requires agencies to develop and implement breach notification policies governing how and under what circumstances affected parties are notified in the event of a data breach. Further, in a memorandum issued in September 2006, OMB recommended that agencies establish a core management group responsible for responding to the loss of personal information.

OMB also established requirements for reporting breaches within the government. In memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB asked agencies to identify in their annual FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information. Agencies are also required to report numbers of incidents for the reporting period, the number of incidents the agency reported to US-CERT, and the number reported to law enforcement.

In 2007 we reported that while requiring agencies to notify affected consumers of a data breach may encourage better security practices and help mitigate potential harm, it also presents certain costs and challenges.[12] Federal banking regulators and the President's Identity Theft Task Force had advocated a notification standard—the conditions requiring notification—that was risk based, allowing individuals to take appropriate measures where the risk of harm existed, while ensuring they are only notified in cases where the level of risk warrants such action. Use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications to consumers about breaches that present little risk.

Data Breaches Continue to Proliferate in the Public and Private Sectors

Over the last several years, we have continued to report that federal agency systems are vulnerable to cyber attacks and the potential compromise of sensitive information, including personally identifiable information.[13] For fiscal year 2011, agency inspector general and GAO assessments of information security controls revealed that most major

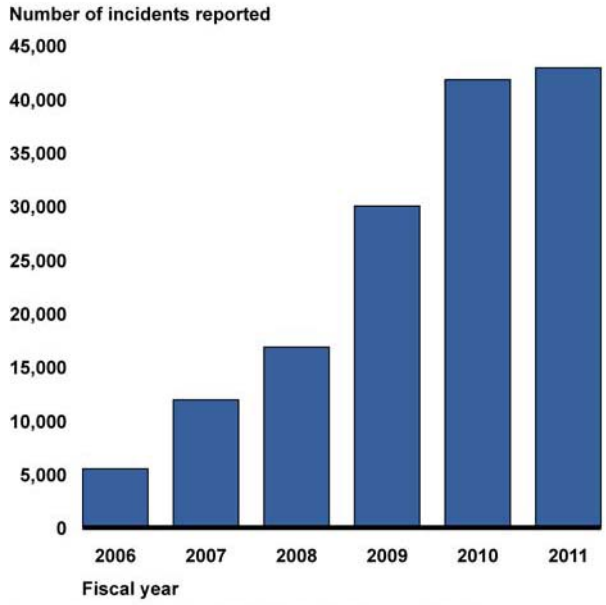
[12]GAO, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, GAO-07-737 (Washington, D.C.: June 4, 2007).

[13]GAO, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137 (Washington, D.C.: Oct. 3, 2011).

federal agencies had weaknesses in most of five major categories of information system controls. Further, over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve similar previously identified significant control deficiencies. We have also recommended that agencies fully implement comprehensive, agency-wide information security programs as required by FISMA, including by correcting weaknesses in specific areas of their programs. The effective implementation of these recommendations will strengthen the security posture at these agencies, which will in turn help ensure the protection of personally identifiable information they collect and use.

Federal agencies have also reported increasing numbers of security incidents that placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Over the past 6 years, the number of incidents reported by federal agencies to US-CERT has increased from 5,503 incidents in fiscal year 2006 to 42,887 incidents in fiscal year 2011, an increase of nearly 680 percent. (See fig. 1.) Of the incidents occurring in 2011, 15,560 involved unauthorized disclosure of personally identifiable information, a 19 percent increase over the 13,017 personally identifiable information incidents that occurred in 2010.

Figure 1: Incidents Reported to US-CERT: Fiscal Years 2006 - 2011



Source: GAO analysis of US-CERT data for fiscal years 2006-2011.

Reported attacks and unintentional incidents involving federal, private and

critical infrastructure systems involve a wide range of incidents including data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples from news media and other public sources illustrate some of the risks:

- In May 2012, the Federal Retirement Thrift Investment Board reported a sophisticated cyber attack on a computer belonging to a third party, which provided services to the Thrift Savings Plan. As a result of the attack, 123,000 participants had their personal information accessed. According to the board, the information accessed included 46,587 individuals' names, addresses, and Social Security numbers, and 79,614 individuals' Social Security numbers and other Thrift Savings Plan-related information.
- In April 2012, hackers breached a server at the Utah Department of Health to access thousands of Medicaid records. Included in the breach were Medicaid recipients and clients of the Children's Health Insurance Plan. About 280,000 people had their Social Security numbers exposed. In addition, another 350,000 people listed in the eligibility inquiries may have had other sensitive data stolen, including names, birth dates, and addresses.
- In March 2012, a news wire service reported that the senior commander of the North Atlantic Treaty Organization (NATO) had been the target of repeated cyber attacks using Facebook that were believed to have originated in China. According to the article, hackers repeatedly tried to dupe those close to the commander by setting up fake Facebook accounts in his name in the hope that his acquaintances would make contact and answer private messages, potentially divulging sensitive information about the commander or themselves.
- In March 2012, it was reported that Blue Cross Blue Shield of Tennessee paid out a settlement of $1.5 million to the U.S. Department of Health and Human Services arising from potential violations stemming from the theft of 57 unencrypted computer hard drives that contained protected health information of over 1 million individuals.

Incidents such as these illustrate that sensitive personally identifiable information remains at risk and that improved protections are needed to ensure the privacy of information collected by the government. While OMB has taken steps through the guidance I described to set requirements for agencies to follow, it is unclear the extent to which all agencies, including smaller agencies such as the Federal Retirement

Thirst Investment Board, are adhering to OMB's guidelines.

In summary, ensuring the privacy and security of personal information collected by the federal government remains a challenge, particularly in light of the increasing dependence on networked information systems that can store, process, and transfer vast amounts of data. These challenges include updating federal laws and guidance to reflect current practices for collecting and using information while striking an appropriate balance between privacy concerns and the government's need to collect information from individuals. They also involve implementing sound practices for securing and applying privacy protection principles to federal systems and the information they contain. Without sufficient attention to these matters, Americans' personally identifiable information remains at risk.

Chairman Akaka, Ranking Member Johnson, and members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include John de Ferrari, Assistant Director; Melina Asencio; Sher'rie Bacon; Anjalique Lawrence; Kathleen Lovett Epperson; Lee McCracken; David Plocher; and Jeffrey Woodward.

Appendix I: Related GAO Products

Cybersecurity: Challenges in Securing the Electricity Grid. GAO-12-926T. Washington, D.C.: July, 17, 2012.

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO-12-130T. Washington, D.C.: October 6, 2011.

Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. GAO-12-137. Washington, D.C.: October 3, 2011.

Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards. GAO-11-751. Washington, D.C.: September 20, 2011.

Data Mining: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism. GAO-11-742. Washington, D.C.: September 7, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO-11-865T. Washington, D.C.: July 26, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities. GAO-11-75. Washington, D.C.: July 25, 2011.

Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain. GAO-11-149. Washington, D.C.: July 8, 2011.

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate. GAO-11-605. Washington, D.C.: Jun 28, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems. GAO-11-463T. Washington, D.C.: March 16, 2011.

High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Information Security: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk. GAO-11-43. Washington, D.C.: November 30, 2010.

Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed. GAO-11-24. Washington, D.C.: October 6, 2010.

Privacy: OPM Should Better Monitor Implementation of Privacy-Related Policies and Procedures for Background Investigations. GAO-10-849. Washington, D.C.: September 7, 2010.

Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies. GAO-10-872T. Washington, D.C.: July 22, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.

Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.

Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing. GAO-10-513. Washington, D.C.: May 27, 2010.

Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies. GAO-10-237. Washington, D.C.: March 12, 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Health Information Technology: HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains. GAO-08-1138, Washington, D.C.: September 17, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Privacy: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information. GAO-08-795T. Washington, D.C.: June 18, 2008.

Privacy: Agencies Should Ensure That Designated Senior Official Have Oversight of Key Functions. GAO-08-603. Washington, D.C.: May 30, 2008.

Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. GAO-08-536. Washington, D.C.: May 19, 2008.

Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy. GAO-07-988T. Washington, D.C.: June 19, 2007.

Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown. GAO-07-737. Washington, D.C.: June 4, 2007.

Privacy: Lessons Learned about Data Breach Notification. GAO-07-657. Washington, D.C.: April 30, 2007.

Homeland Security: Continuing Attention to Privacy Concerns Is Needed as Programs Are Developed. GAO-07-630T. Washington, D.C.: March 21, 2007.

Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy. GAO-07-238. Washington, D.C.: January 10, 2007.

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

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