United States Government Accountability Office

GAO

Testimony

Committee on Government Reform,
House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
Thursday, June 8, 2006

PRIVACY

Preventing and Responding to Improper Disclosures of Personal Information

Statement of David M. Walker
Comptroller General of the United States

GAO-06-833T

June 8, 2006

PRIVACY

Preventing and Responding to Improper Disclosures of Personal Information

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-833T, a testimony before the Committee on Government Reform, House of Representatives

Why GAO Did This Study

The recent security breach at the Department of Veterans Affairs, in which personal data on millions of veterans were compromised, has highlighted the importance of the federal government's processes for protecting personal information. As the federal government obtains and processes information about individuals in increasingly diverse ways, it remains critically important that it properly protect this information and respect the privacy rights of individuals.

GAO was asked to testify on preventing and responding to improper disclosures of personal information in the federal government, including how agencies should notify individuals and the public when breaches occur. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources.

What GAO Recommends

GAO has made recommendations previously to agencies and to the Office of Management and Budget (OMB), which provides guidance to agencies on implementing federal privacy and security laws, to ensure that they are adequately addressing security and privacy issues.
In addition, in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-833T.

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

Agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. Two key steps are as follows:

- Develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. These assessments, required by the E-Government Act of 2002, 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 that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (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.

More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting the time that 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.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Although existing laws do not require agencies to notify the public when data breaches occur, 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. That said, care is needed in defining appropriate criteria for incidents that merit notification. Notifying individuals of security incidents that do not pose serious risks could be counterproductive and costly, while giving too much discretion to agencies could result in their avoiding the disclosure of potentially harmful breaches. Care is also needed to ensure that notices are useful and easy to understand, so that they are effective in alerting recipients to actions they may want to take to minimize the risk of identity theft. Among other things, it is important to provide context in the notice—explaining to recipients why they are receiving a notice and what to do about it. It is also important the notices be coordinated with law enforcement to avoid impeding ongoing investigations. Given that individuals may be adversely impacted by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.

Mr. Chairman and Members of the Committee:

I appreciate the opportunity to be here today to discuss key challenges federal agencies face in safeguarding personally identifiable information[1] in their custody and taking action when that information is compromised. As the federal government obtains and processes personal information about individuals in increasingly diverse ways, it remains critically important that this information be properly protected and the privacy rights of individuals respected. Recently, as you know, personal data on millions of veterans was stolen from the home of an employee of the Department of Veterans Affairs, who had not been authorized to have the data at home. Compromises such as this raise important questions about what steps agencies should take to prevent such compromises and how they should notify citizens when breaches do occur.

As requested, my statement will focus on preventing and responding to improper disclosures of personal information in the federal government, including notifying the public about such security breaches. After a brief summary and discussion of the federal laws and guidance that apply to agency use of personal information, I will discuss potential measures that federal agencies can take to help limit the likelihood of personal information being compromised and then highlight key benefits and challenges associated with effectively notifying the public about security breaches.

To address measures that agencies can take to help limit the likelihood of personal information being compromised, we identified and summarized issues raised by experts in congressional testimony and in our previous reports, including our recent work regarding the federal government's use of personal information from

[1] For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including both identifiable and nonidentifying information. *Personally identifiable information*, which can be used to locate or identify an individual, includes such things as names, aliases, and Social Security numbers. *Nonidentifying personal information* includes such things as age, education, finances, criminal history, physical attributes, and gender.

companies known as information resellers.[2] We conducted the work for these reports in accordance with generally accepted government auditing standards. To identify benefits and challenges associated with effectively notifying the public about security breaches, we summarized expert opinion from congressional testimony as well as key practices identified at a Department of Homeland Security (DHS) privacy workshop, by the state of California, and by the Federal Trade Commission. To provide additional information on our previous privacy-related work, I have included, as an attachment, a list of 20 pertinent GAO publications.

Results in Brief

Agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. Two key steps are (1) to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed in a federal information system—whenever information technology is used to process personal information and (2) to ensure that a robust information security program is in place, as required by the Federal Information Security Management Act of 2002 (FISMA). More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting access to personal information and training personnel accordingly, and considering using technological controls such as encryption when data need to be stored on mobile devices.

When data breaches do occur, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. It is also consistent with agencies' responsibility to inform individuals about how their information is being accessed

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

and used and promotes accountability for its protection. At the same time, concerns have been raised that notifying individuals of security incidents that do not pose serious risks could be counterproductive and costly. Care is needed in defining appropriate criteria if agencies are required to report security breaches to the public, including coordinating with law enforcement. Care is also needed to ensure that notices are useful and easy to understand so that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

We have made recommendations previously to OMB and agencies to ensure they are adequately addressing privacy issues, including through the conduct of privacy impact assessments. We have also recommended that OMB implement improvements in its annual FISMA reporting guidance to help improve oversight of agency information security programs. In addition, the Congress should consider setting specific reporting requirements for agencies as part of its consideration of security breach legislation. Further Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Background

The recent theft of personally identifiable information on millions of veterans is only the latest of a series of such data breaches involving the loss or theft of information on magnetic tapes, computer hard drives, and other devices, as well as incidents in which individuals gained unauthorized access to large commercial databases of such information. Concerns about possible identity theft resulting from such breaches are widespread. The Federal Trade Commission (FTC) reported in 2005 that identity theft represented about 40 percent of all the consumer fraud complaints it received during each of the last 3 calendar years. Identity theft generally involves the fraudulent use of another person's identifying information—such as name, address, Social Security number, date of birth, or mother's maiden name—to establish credit, run up debt, or take over existing

financial accounts. According to identity theft experts, individuals whose identities have been stolen can spend months or years and thousands of dollars clearing their names. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft.

Several Key Laws Govern Agency Privacy Practices

Federal agencies are subject to security and privacy laws aimed in part at preventing security breaches, including breaches that could enable identity theft. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the E-Government 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.[3] Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes.

The Office of Management and Budget (OMB), which is responsible for providing guidance to agencies on how to implement the

[3] 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).

provisions of the Privacy Act and other federal privacy and security laws, recently issued a memorandum reminding agencies of their responsibilities under the Privacy Act, other laws, and policy to appropriately safeguard sensitive personally identifiable information and train employees on their responsibilities in this area.[4] The memo called on agency senior privacy officials to conduct a review of policies and processes to make sure adequate safeguards are in place to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

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;[5] 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 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 OMB guidance,[6] a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements

[4] Office of Management and Budget, *Safeguarding Personally Identifiable Information*, M-06-15 (Washington, D.C.: May 22, 2006).

[5] 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).

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

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. To the extent that PIAs are made publicly available,[7] 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. FISMA 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.[8] 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, among other things. Your committee has issued annual report cards on federal government information security based on reports submitted by agencies as required by FISMA.

Interest in Data Breach Notification Legislation Has Increased

Federal laws to date have not required agencies to report security breaches to the public,[9] although breach notification has played an important role in the context of security breaches in the private sector. For example, California state law requires businesses to notify consumers about security breaches that could directly affect

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

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

[9] At least one agency has developed its own requirement for breach notification. Specifically, the Department of Defense instituted a policy in July 2005 requiring notification to affected individuals when protected personal information is lost, stolen, or compromised.

them. Legal requirements, such as the California law, led ChoicePoint, a large information reseller,[10] to notify its customers in mid-February 2005 of a security breach in which unauthorized persons gained access to personal information from its databases. Since the ChoicePoint notification, bills were introduced in at least 44 states and enacted in at least 29[11] that require some form of notification upon a security breach.

A number of congressional hearings were held and bills introduced in 2005 in the wake of the ChoicePoint security breach as well as incidents at other firms. In March 2005, the House Subcommittee on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Committee held a hearing entitled "Protecting Consumers' Data: Policy Issues Raised by ChoicePoint," which focused on potential remedies for security and privacy concerns regarding information resellers. Similar hearings were held by the House Energy and Commerce Committee and by the U.S. Senate Committee on Commerce, Science, and Transportation in spring 2005.

Several bills introduced at the time of these hearings, such as the Data Accountability and Trust Act,[12] would establish a national requirement for companies that maintain personal information to notify the public of security breaches. While many of these proposals were focused on private sector companies rather than the federal government, they could be applied to any organizations that collect and maintain significant amounts of personally identifiable information. The Notification of Risk to Personal Data Act[13] would

[10] 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. For additional information, see GAO-06-421.

[11] States that have enacted breach notification laws include Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin.

[12] H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

[13] S. 751; introduced by Senator Dianne Feinstein on April 11, 2005.

explicitly include federal agencies, requiring them as well as any "persons engaged in interstate commerce" to disclose security breaches involving unauthorized acquisition of personal data.

Agencies Can Take Steps to Reduce the Likelihood That Personal Data Will Be Compromised

A number of actions can be taken to help guard against the possibility that personal information maintained by agencies is inadvertently compromised. I will focus my remarks today on key strategic approaches for safeguarding personal information as well as a few practical measures that could be critical in preventing data breaches. I will not discuss at length the broader topic of information security in the federal government, which both the committee and GAO have addressed extensively in the past.[14] Key strategic approaches include the following:

Conduct privacy impact assessments (PIAs). It is important that agencies identify the specific instances in which they collect and maintain personal information and proactively assess the means they intend to use to protect this information. This can be done most effectively through the development of PIAs, which, as I previously mentioned, are required by the E-Government Act of 2002 when using information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments.

In prior work we have found that agencies do not always prepare PIAs as they are required. For example, our review of selected data

[14] See, for example, GAO, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267 (Washington, D.C.: February 24, 2006) and *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program*, GAO-05-700 (Washington, D.C.: June 17, 2005).

mining efforts at federal agencies[15] determined that PIAs were not always being done in full compliance with OMB guidance. Similarly, as identified in our work on federal agency use of information resellers,[16] few PIAs were being developed for systems or programs that made use of information reseller data because officials did not believe they were required. Complete assessments are an important tool for agencies to identify areas of noncompliance with federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy of personal information risk the improper exposure or alteration of such information. We recommended that the agencies responsible for the data mining efforts we reviewed complete or revise PIAs as needed and make them available to the public. We also recommended that OMB revise its guidance to clarify the applicability of the E-Gov Act's PIA requirement to the use of personal information from resellers. OMB stated that it would discuss its guidance with agency senior officials for privacy to determine whether additional guidance concerning reseller data was needed.

Ensure that a robust security program is in place. FISMA requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Key elements of this program include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

[15] GAO, *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).

[16] GAO-06-421, pp. 59–61.

- risk-based policies and procedures that cost-effectively reduce risks to an acceptable level and ensure that security is addressed throughout the life cycle of each information system;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies through plans of action and milestones; and
- procedures for detecting, reporting, and responding to security incidents.

In prior reviews we have repeatedly identified weaknesses in almost all areas of information security controls at major federal agencies, and we have identified information security as a high risk area across the federal government since 1997. In July 2005, we reported that pervasive weaknesses in the 24 major agencies' information security policies and practices threatened the integrity, confidentiality, and availability of federal information and information systems.[17] These weaknesses existed primarily because agencies had not yet fully implemented strong information security management programs, as needed to fully meet FISMA requirements. We recommended that OMB implement improvements in its annual FISMA reporting guidance to help improve oversight of agency information security programs. In March 2006, we reported that OMB had taken several actions to improve reporting and could further enhance the reliability and quality of reported information.[18]

[17] GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[18] GAO, *Information Security: Federal Agencies Show Mixed Progress In Implementing Statutory Requirements*, GAO-06-527T (Washington, D.C.: March 16, 2006).

In the course of taking strategic approaches to protecting the privacy and security of personal information, agencies will likely consider a range of specific practical measures. Several that may be of particular value in preventing inadvertent data breaches include the following:

Limit collection of personal information. One item to be analyzed as part of a PIA is the extent to which an agency needs to collect personal information in order to meet the needs of a specific application. Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information—such as Social Security numbers—may not be needed for many agency applications that have databases of other personal information. Limiting the collection of personal information is also one of the fair information practices, which are fundamental to the Privacy Act and to good privacy practice in general.

Limit data retention. Closely related to limiting data collection is limiting retention. Retaining personal data longer than needed by an agency or statutorily required adds to the risk that the data will be compromised. In discussing data retention, California's Office of Privacy Protection recently reported an example in which a university experienced a security breach that exposed 15-year-old data, including Social Security numbers. The university subsequently reviewed its policies and decided to shorten the retention period for certain types of information.[19] Federal agencies can make decisions up front about how long they plan to retain personal data as part of their PIAs, aiming to retain the data for as brief a period as necessary.

Limit access to personal information and train personnel accordingly. Only individuals with a need to access agency databases of personal information should have such access, and controls should be in place to monitor that access. Further, agencies can implement technological controls to prevent personal data from being readily transferred to unauthorized systems or media, such as

[19] State of California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information* (April 2006), p. 6.

laptop computers, discs, or other electronic storage devices. Security training, which is required for all federal employees under FISMA, can include training on the risks of exposing personal data to potential identity theft, thus helping to reduce the likelihood of data being exposed inadvertently.

Consider using technological controls such as encryption when data needs to be stored on mobile devices. In certain instances, agencies may find it necessary to enable employees to have access to personal data on mobile devices such as laptop computers. As discussed, this should be minimized. However, when absolutely necessary, the risk that such data could be exposed to unauthorized individuals can be reduced by using technological controls such as encryption, which significantly limits the ability of such individuals gaining access to the data. While encrypting data adds to the operational burden on authorized individuals, who must enter pass codes or use other authentication means to decrypt the data, it can provide reasonable assurance that stolen or lost computer equipment will not result in personal data being compromised, as occurred in the recent incident at the Department of Veterans Affairs. A decision about whether to use encryption would logically be made as an element of the PIA process and an agency's broader information security program.

While these suggestions do not amount to a complete prescription for protecting personal data, they are key elements of an agency's strategy for reducing the risks that could lead to identity theft.

Public Notification of Data Breaches Has Clear Benefits as Well as Challenges

I just discussed some preventive measures agencies can take to avoid a data breach. However, in the event an incident does occur, agencies must respond quickly in order to minimize the potential harm associated with identity theft. Applicable laws such as the Privacy Act currently do not require agencies to notify individuals of security breaches involving their personal information; however, doing so allows those affected the opportunity to take steps to protect themselves against the dangers of identity theft. For

example, the California data breach notification law is credited with bringing to the public's notice large data breaches within the private sector, including at information resellers such as ChoicePoint and LexisNexis last year. Although we do not know how many instances of identity theft resulted from last year's data breaches, the Federal Trade Commission has previously reported that the overall cost of an incident of identity theft, as well as the harm to the victims, is significantly smaller if the misuse of the victim's personal information is discovered quickly.[20] Arguably, the California law may have mitigated the risk of identity theft to affected individuals by keeping them informed about data breaches and thus enabling them to take steps such as contacting credit bureaus to have fraud alerts placed on their credit files, obtaining copies of their credit reports, scrutinizing their monthly financial account statements, and taking other steps to protect themselves. The chairman of the Federal Trade Commission has testified that the Commission believes that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified.[21]

Breach notification is also important in that it can help an organization address key privacy rights of individuals. These rights are based on the fair information practices (see attachment 2); these principles have been widely adopted and are the basis of privacy laws and related policies in many countries, including the United States. In particular, the *openness* principle states that the public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information. Breach notification is one way that organizations—either in the private sector or the government—can meet their responsibility for keeping the public informed of how their personal information is being used and who has access to it. Equally important is the *accountability* principle, which states that individuals controlling the collection or use of personal information

[20] Synovate, *Federal Trade Commission Identity Theft Survey Report* (McLean, Va.: September 2003).

[21] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10.

should be accountable for taking steps to ensure the implementation of the other principles, such as use limitation and security safeguards. Public disclosure of data breaches is a key step in ensuring that organizations are held accountable for the protection of personal information.

Concerns Have Been Raised About the Criteria for Issuing Notices to the Public

Although the principle of notifying affected individuals (or the public) about data breaches has clear benefits, determining the specifics of when and how an agency should issue such notifications presents challenges, particularly in determining the specific criteria for incidents that merit notification. In congressional testimony, the Federal Trade Commission[22] raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects. First, notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Second, a surfeit of notices, resulting from notification criteria that are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant. Finally, the costs to both individuals and business are not insignificant and may be worth considering. The FTC points out that, in response to a security breach notification, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on credit files, or obtain a new driver's license number. These actions could be time-consuming for the individual and costly for the companies involved. Given these potential negative effects, care is clearly needed in defining appropriate criteria for required breach notifications.

While care needs to be taken to avoid requiring agencies to notify the public of trivial security incidents, concerns have also been raised about setting criteria that are too open-ended or that rely too heavily on the discretion of the affected organization. Some public advocacy groups have cautioned that notification criteria that are

[22] Federal Trade Commission, *Prepared Statement on Data Breaches and Identity Theft*, p. 10.

too weak would give companies an incentive not to disclose potentially harmful breaches. This concern could also apply to federal agencies. In congressional testimony last year, the executive director of the Center for Democracy and Technology argued that if an entity is not certain whether a breach warrants notification, it should be able to consult with the Federal Trade Commission.[23] He went on to suggest that a two-tiered system may be desirable, with notice to the Federal Trade Commission of all breaches of personal data and notice to consumers where there is a potential risk of identity theft. The Center for Democracy and Technology's comments regarding the Federal Trade Commission were aimed at commercial entities such as information resellers. A different entity—such as OMB, which is responsible for overseeing security and privacy within the federal government—might be more appropriate to take on a parallel role with respect to federal agencies.

Effective Notices Should Provide Useful Information and Be Easy to Understand

Once a determination has been made that a public notice is to be issued, care must be taken to ensure that it does its job effectively. Designing useful, easy-to-understand notices has been cited as a challenge in other areas where privacy notices are required by law, such as in the financial industry—where businesses are required by the Gramm-Leach-Bliley Act to send notices to consumers about their privacy practices—and in the federal government, which is required by the Privacy Act to issue public notices in the *Federal Register* about its systems of records containing personal information. For example, as noted during a public workshop hosted by the Department of Homeland Security's Privacy Office, designing easy-to-understand consumer financial privacy notices to meet Gramm-Leach Bliley Act requirements has been challenging. Officials from the FTC and Office of the Comptroller of the Currency described widespread criticism of these notices—that they were unexpected, too long, filled with legalese, and not understandable.

[23] Center for Democracy and Technology, *Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Government Use* (Apr. 13, 2005), p. 7.

If an agency is to notify people of a data breach, it should do so in such a way that they understand the nature of the threat and what steps need to be taken to protect themselves against identity theft. In connection with its state law requiring security breach notifications, the California Office of Privacy Protection has published recommended practices for designing and issuing security breach notices.[24] The office recommends that such notifications include, among other things,

- a general description of what happened;
- the type of personal information that was involved;
- what steps have been taken to prevent further unauthorized acquisition of personal information;
- the types of assistance to be provided to individuals, such as a toll-free contact telephone number for additional information and assistance;
- information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies; and
- information on where individuals can obtain additional information on protection against identity theft, such as the Federal Trade Commission's Identity Theft Web site (www.consumer.gov/idtheft).

The California Office of Privacy Protection also recommends making notices clear, conspicuous, and helpful, by using clear, simple language and avoiding jargon and suggests avoiding using a standardized format to mitigate the risk that the public will become complacent about the process.

The Federal Trade Commission has issued guidance to businesses on notifying individuals of data breaches that reiterates several key elements of effective notification—describing clearly what is known about the data compromise, explaining what responses may be appropriate for the type of information taken, and providing information and contacts regarding identity theft in general. The

[24] State of California, *Recommended Practices on Notice of Security Breach.*

Commission also suggests providing contact information for the law enforcement officer working on the case as well as encouraging individuals who discover that their information has been misused to file a complaint with the Commission.[25]

Both the state of California and the Federal Trade Commission recommend consulting with cognizant law-enforcement officers about an incident before issuing notices to the public. In some cases, early notification or disclosure of certain facts about an incident could hamper a law enforcement investigation. For example, an otherwise unknowing thief could learn of the potential value of data stored on a laptop computer that was originally stolen purely for the value of the hardware. Thus it is recommended that organizations consult with law enforcement regarding the timing and content of notifications. However, law enforcement investigations should not necessarily result in lengthy delays in notification. California's guidance states that it should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

During a recent public workshop on "Transparency and Accountability: The Use of Personal Information within the Government," hosted by the DHS Privacy Office, a panelist discussed the concept of "layering" notices to foster greater understanding and comprehension by consumers. Layering involves providing only the most important summary facts up front—often in a graphically oriented format—followed by one or more lengthier, more narrative versions in order to ensure that all information is communicated that needs to be. The panelist noted the pros and cons of lengthy, detailed notices versus brief, easier-to-understand notices. Specifically, long notices have the advantage of being complete, but this is often at a cost of not being easy to understand, while brief, easier-to-understand notices may not capture all the detail that needs to be conveyed. Multilayered notices were cited as an option to achieving an easy-to-understand yet complete notice.

[25] Federal Trade Commission, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* (June 2004).

In addition, DHS workshop panelists from the Federal Trade Commission and the Office of the Comptroller of the Currency discussed the major findings of an interagency research project[26] concerning the design of easy-to-understand consumer financial privacy notices. The study found, among other things, that providing context to the notice (explaining to consumers why they are receiving the notice and what to do with it) was key to comprehension, and that comprehension was aided by incorporating key visual design elements, such as use of a tabular format, large and legible fonts, and appropriate use of white space and simple headings.

Although these panel discussions were not focused on notices to inform the public of data breaches, the multilayered approach discussed and findings from the interagency research project can be applied to such notices. For example, a multilayered security breach notice could include a brief description of the nature of the security breach, the potential threat to victims of the incident, and measures to be taken to protect against identity theft. The notice could provide additional details about the incident as an attachment or by providing links to additional information. This would accomplish the purpose of communicating the key details in a brief format, while still providing complete information to those who require it. Given that people may be adversely affected by a compromise of their personal information, it is critical that they fully understand the nature of the threat and the options they have to address it.

In summary, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised, among which developing PIAs and ensuring that a robust information security program is in place are key. More specific practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal information, limiting data retention, limiting

[26] Kleimann Communication Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006).

access to personal information and training personnel accordingly, and considering using technological controls such as encryption when data need to be stored on mobile devices. Nevertheless, data breaches can still occur at any time, and when they do, notification to the individuals affected and/or the public has clear benefits, allowing people the opportunity to take steps to protect themselves against the dangers of identity theft. Care is needed in defining appropriate criteria if agencies are to be required to report security breaches to the public. Further, care is also needed to ensure that notices are useful and easy-to-understand so that they are effective in alerting individuals to actions they may want to take to minimize the risk of identity theft.

As Congress considers legislation requiring agencies to notify individuals or the public about security breaches, it should ensure that specific criteria are defined for incidents that merit public notification. It may want to consider creating a two-tier reporting requirement, in which all security breaches are reported to OMB, and affected individuals are notified only of incidents involving significant risk. Further, Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Mr. Chairman, this concludes my testimony today. I would happy to answer any questions you or other members of the committee 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 Idris Adjerid, Barbara Collier, John de Ferrari, David Plocher, and Jamie Pressman.

Attachment I: Selected GAO Products Related to Privacy Issues

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 Security: Federal Agencies Show Mixed Progress In Implementing Statutory Requirements. GAO-06-527T. Washington, D.C.: March 16, 2006.

Information Security: Department of Health and Human Services Needs to Fully Implement Its Program. GAO-06-267. Washington, D.C.: February 24, 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.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO-05-552. Washington, D.C.: July 15, 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: Department of Homeland Security Needs to Fully Implement Its Security Program. GAO-05-700. Washington, D.C.: June 17, 2005.

Electronic Government: Federal Agencies Have Made Progress Implementing the E-Government Act of 2002. GAO-05-12. Washington, D.C.: December 10, 2004.

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.

Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges, GAO-04-823. Washington, D.C.: July 21, 2004.

Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548. Washington, D.C.: May 4, 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[27] 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.

[27] 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.

(310768)

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