



Testimony
Before the Committee on Veterans'
Affairs, House of Representatives

For Release on Delivery
Expected at time 10:30 a.m. EDT
June 14, 2006

VETERANS AFFAIRS

Leadership Needed to Address Information Security Weaknesses and Privacy Issues

Statement of Linda D. Koontz
Director, Information Management Issues

and

Gregory C. Wilshusen
Director, Information Security Issues



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-06-866T](#), a testimony before the Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals.

GAO was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. 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

To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

www.gao.gov/cgi-bin/getrpt?GAO-06-866T.

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.

VETERANS AFFAIRS

Leadership Needed to Address Information Security Weaknesses and Privacy Issues

What GAO Found

For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. Both GAO and the department's inspector general have reported recurring weaknesses in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced.

In addition to establishing robust security programs, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. A key step is to 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. In addition, agencies can take more specific practical measures aimed at preventing data breaches, including 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 portable devices.

When data breaches do occur, notification of those affected and/or the public has clear benefits, allowing people the opportunity to protect themselves from identity theft. Although existing laws do not require agencies to notify the public of data breaches, 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 triggering notification. Notices should be coordinated with law enforcement to avoid impeding ongoing investigations, and in order to be effective, notices should be easy to understand. Because of the possible adverse impact of a compromise of personal information, it is critical that people fully understand the threat and their options for addressing it.

Strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight will be needed for VA to address its persistent, long-standing control weaknesses.

Mr. Chairman and Members of the Committee:

Thank you for inviting us to participate in today's hearing on information security and privacy at the Department of Veterans Affairs (VA). For many years, we have identified information security as a governmentwide high-risk issue¹ and emphasized its criticality for protecting the government's information assets. The recent security breach at VA, involving the loss of personal data on millions of veterans, also raises important questions about the protection of personally identifiable information.²

Today we will first address VA's information security program, including weaknesses reported by us and others, as well as actions that VA has taken to address past recommendations in this area. We will then discuss potential measures that federal agencies can take to help limit the likelihood of personal information being compromised. Finally, we will highlight key benefits and challenges associated with effectively notifying the public about security breaches.

To describe VA's information security weaknesses, we reviewed our previous work in this area, as well as reports by VA's inspector general (IG) and others. To determine the implementation status of our open recommendations, we analyzed VA documentation and met with officials from VA, including security and IG officials. 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 companies

¹ GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005) and *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, [GAO-05-552](#) (Washington, D.C.: July 15, 2005).

² 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.

known as information resellers.³ To identify benefits and challenges associated with effectively notifying the public about security breaches, we reviewed our previous work in this area. We conducted the work for our previous reports in accordance with generally accepted government auditing standards. To provide additional information on our previous work related to VA security issues and to privacy, we have included, as an attachment, a list of pertinent GAO publications.

Results in Brief

Significant concerns have been raised over the years about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information. We have previously reported on wide-ranging deficiencies in VA's information security controls.⁴ For example, the department lacked effective controls to prevent individuals from gaining unauthorized access to VA systems and sensitive information, and it had not consistently provided adequate physical security for its computer facilities, assigned duties in a manner that segregated incompatible functions, controlled changes to its operating systems, or updated and tested its disaster recovery plans. These deficiencies existed, in part, because VA had not fully implemented key components of a comprehensive, integrated information security program. Although VA has taken steps to implement components of its security program, its efforts have not been sufficient to effectively protect its information and information systems. As a result, sensitive information, including personally identifiable information, remains vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure, as the recent breach demonstrates.

³ GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington: D.C.: Apr. 4, 2006).

⁴ See attachment 1.

In addition to establishing a robust information security program, agencies can take a number of actions to help protect personally identifiable information from compromise. A key step is 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. In addition, 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 the use of technological controls such as encryption when data need to be stored on portable 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 and used, and promotes accountability for its protection. If agencies are required to report security breaches to the public, care will be needed to develop appropriate criteria for incidents that require notification. 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 VA regarding information security and to the Office of Management and Budget (OMB) and agencies regarding privacy issues, including the conduct of privacy impact assessments. In addition, we have previously testified that the Congress should consider setting specific reporting requirements for agencies as part of its consideration of security breach legislation. Further, the Congress should consider requiring OMB to provide guidance to agencies on how to develop and issue security breach notices to affected individuals.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous, but without proper safeguards in the form of appropriate information security, this widespread interconnectivity also poses significant risks to the government’s computer systems and the critical operations and infrastructures they support.

In prior reviews we have repeatedly identified weaknesses in almost all areas of information security controls at major federal agencies, including VA, 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.⁵ As we reported, although federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. These weaknesses existed primarily because agencies had not yet fully implemented strong information security programs, as required by the Federal Information Security Management Act (FISMA).

The significance of these weaknesses led us to conclude in the audit of the federal government’s fiscal year 2005 financial statements⁶

⁵ 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).

⁶ U.S. Department of the Treasury, *Financial Report of the United States Government 2005* (Washington, D.C.: 2005).

that information security was a material weakness.⁷ Our audits also identified instances of similar types of weaknesses in nonfinancial systems. Weaknesses continued to be reported in each of the major areas of *general controls*: that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.⁸

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, without which agencies would find it difficult, if not impossible, to carry out their missions and account for their resources. The following examples show the broad array of federal operations and assets placed at risk by information security weaknesses:

- Resources, such as federal payments and collections, could be lost or stolen.
- Computer resources could be used for unauthorized purposes or to launch attacks on others.
- Personal information, such as taxpayer data, social security records, and medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of identity theft, industrial espionage, or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud, theft of assets, or disruption.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

⁷ A material weakness is a condition that precludes the entity's internal control from providing reasonable assurance that misstatements, losses, or noncompliance that is material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

⁸ The main areas of general controls are an agencywide security program, access controls, software change controls, segregation of duties, and continuity of operations planning.

The potential disclosure of personal information raises additional identity theft and privacy concerns. Identity theft generally involves the fraudulent use of another person's identifying information—such as 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. 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. Beyond the serious issues surrounding identity theft, the unauthorized disclosure of personal information also represents a breach of individuals' privacy rights to have control over their own information and to be aware of who has access to this information.

Key Laws Govern Agency Security and 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.

FISMA is the primary law governing information security in the federal government; it also addresses the protection of personal information in the context of securing federal agency information and information systems. The act defines federal requirements for securing information and information systems that support federal agency operations and assets.⁹ Under FISMA, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure (and thus to protect personal privacy, among other things). The act requires each agency to develop, document, and implement an agencywide information security program to provide

⁹ FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002).

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.

FISMA describes a comprehensive information security program as including the following elements:

- 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;
- 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 particular, FISMA requires that for any information they hold, agencies evaluate the associated risk according to three categories: (1) confidentiality, which is the risk associated with unauthorized disclosure of the information; (2) integrity, the risk of unauthorized modification or destruction of the information; and (3) availability, which is the risk of disruption of access to or use of information. Thus, each agency should assess the risk associated with personal data held by the agency and develop appropriate protections.

The agency can use this risk assessment to determine the appropriate controls (operational, technical, and managerial) that will reduce the risk to an acceptably low level. For example, if an agency assesses the confidentiality risk of the personal information as high, the agency could create control mechanisms to help protect the data from unauthorized disclosure. Besides appropriate policies,

these controls would include access controls and monitoring systems:

- Access controls are key technical controls to protect the confidentiality of information. Organizations use these controls to grant employees the authority to read or modify only the information the employees need to perform their duties. In addition, access controls can limit the activities that an employee can perform on data. For example, an employee may be given the right to read data, but not to modify or copy it. Assignment of rights and permissions must be carefully considered to avoid giving users unnecessary access to sensitive files and directories.
- To ensure that controls are, in fact, implemented and that no violations have occurred, agencies need to monitor compliance with security policies and investigate security violations. It is crucial to determine what, when, and by whom specific actions are taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security events.

A comprehensive security program of the type described is a prerequisite for the protection of personally identifiable information held by agencies. In addition, agencies are subject to requirements specifically related to personal privacy protection, which come primarily from two laws, the Privacy Act of 1974 and 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. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act

requires that when agencies establish or make changes to a system of records, they must notify the public by a “system-of-records notice”: that is, a notice in the *Federal Register* identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended “routine” uses of data, and procedures that individuals can use to review and correct personal information.¹⁰ Among other provisions, the act also requires agencies to define and limit themselves to specific predefined purposes.

The provisions of the Privacy Act are consistent with and largely based on a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices,¹¹ which have been widely adopted as a standard benchmark for evaluating the adequacy of privacy protections; they include such principles as openness (keeping the public informed about privacy policies and practices) and accountability (those controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles).

- 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,¹² a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in

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

¹¹ These principles were first proposed in 1973 by a U.S. government advisory committee; they were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. Congress used the committee’s final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

¹² Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

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,¹³ they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

Interest in Data Breach Notification Legislation Has Increased

Federal laws to date have not required agencies to report security breaches to the public,¹⁴ although breach notification has played an important role in the context of security breaches in the private sector. For example, requirements of California state law led ChoicePoint, a large information reseller,¹⁵ to notify its customers of a security breach in February 2005. Since the ChoicePoint notification, bills were introduced in at least 44 states and enacted in at least 29¹⁶ 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

¹³ 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).

¹⁴ 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.

¹⁵ 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](#).

¹⁶ 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.

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 (DATA),¹⁷ would establish a national requirement for companies that maintain personal information to notify the public of security breaches. In May 2006, DATA was amended to also require federal agencies to notify citizens and residents of the United States whose personal information is acquired by an unauthorized person as a result of a security breach. Other bills under consideration also include federal agencies. For example, the Notification of Risk to Personal Data Act¹⁸ would require federal agencies as well as any “persons engaged in interstate commerce” to disclose security breaches involving unauthorized acquisition of personal data.

VA’s Information Security Is Weak

Our previous reports and testimonies describe numerous weaknesses in VA’s information security controls. Although the department has taken steps to address these weaknesses, they have not been sufficient to fully implement a comprehensive, integrated information security program and to fully protect VA’s information and information systems. As a result, these remain at risk.

VA’s Information Security Weaknesses Are Long Standing

In carrying out its mission of providing health care and benefits to veterans, VA relies on a vast array of computer systems and

¹⁷ H.R. 4127; introduced by Representative Clifford B. Stearns on October 25, 2005.

¹⁸ S. 751; introduced by Senator Dianne Feinstein on April 11, 2005.

telecommunications networks to support its operations and store sensitive information, including personal information on veterans. VA's networks are highly interconnected, its systems support many users, and the department has increasingly moved to more interactive, Web-based services to better meet the needs of its customers. Effectively securing these computer systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive veterans' health and disability benefits information, and ensure the integrity of its financial data.

In this complex IT environment, VA has faced long-standing challenges in achieving effective information security across the department. Our reviews¹⁹ identified wide-ranging, often recurring deficiencies in the department's information security controls (attachment 2 provides further detail on our reports and the areas of weakness they discuss). Examples of areas of deficiency include the following.

- *Access authority was not appropriately controlled.* A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Electronic access controls are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information and include controls related to user accounts and passwords, user rights and file permissions, logging and monitoring of security-relevant events, and network management. Inadequate controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service.

However, VA had not established effective electronic access controls to prevent individuals from gaining unauthorized access to its systems and sensitive data, as the following examples illustrate:

- *User accounts and passwords:* In 1998, many user accounts at four VA medical centers and data centers had weaknesses

¹⁹ Attachment 1 includes a list of our products related to IT vulnerabilities at VA.

including passwords that could be easily guessed, null passwords, and passwords that were set to never expire. We also found numerous instances where medical and data center staff members were sharing user IDs and passwords.

- *User rights and permissions:* We reported in 2000 that three VA health care systems were not ensuring that user accounts with broad access to financial and sensitive veteran information had proper authorization for such access, and were not reviewing these accounts to determine if their level of access remained appropriate.
- *Logging and monitoring of security-related events:* In 1998, VA did not have any departmentwide guidance for monitoring both successful and unsuccessful attempts to access system files containing key financial information or sensitive veteran data, and none of the medical and data centers we visited were actively monitoring network access activity. In 1999, we found that one data center was monitoring failed access attempts, but was not monitoring successful accesses to sensitive data and resources for unusual or suspicious activity.
- *Network management:* In 2000, we reported that one of the health care systems we visited had not configured a network parameter to effectively prevent unauthorized access to a network system; this same health care system had also failed to keep its network system software up to date.
- *Physical security controls were inadequate.* Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. VA had weaknesses in the physical security for its computer facilities. For example, in our 1998 and 2000 reports, we stated that none of the VA facilities we visited were adequately controlling access to their computer rooms. In addition, in 1998 we reported that sensitive equipment at two facilities was not adequately protected, increasing the risk of disruption to computer operations or network communications.

-
- *Employees were not prevented from performing incompatible duties.* Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation. Dividing duties among two or more individuals or organizational groups diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. We determined that VA did not assign employee duties and responsibilities in a manner that segregated incompatible functions among individuals or groups of individuals. For example, in 1998 we reported that some system programmers also had security administrator privileges, giving them the ability to eliminate any evidence of their activity in the system. In 2000, we reported that two VA health care systems allowed some employees to request, approve, and receive medical items without management approval, violating both basic segregation of duties principles and VA policy; in addition, no mitigating controls were found to alert management of purchases made in this manner.
 - *Software change control procedures were not consistently implemented.* It is important to ensure that only authorized and fully tested systems are placed in operation. To ensure that changes to systems are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. We found that VA did not adequately control changes to its operating systems. For example, in 1998 we reported that one VA data center had not established detailed written procedures or formal guidance for modifying operating system software, for approving and testing operating system software changes, or for implementing these changes. The data center had made more than 100 system software changes during fiscal year 1997, but none of the changes included evidence of testing, independent review, or acceptance. We reported in 2000 that two VA health care systems had not established procedures for periodically reviewing changes to standard application programs to ensure that only authorized program code was implemented.

-
- *Service continuity planning was not complete.* In addition to protecting data and programs from misuse, organizations must also ensure that they are adequately prepared to cope with a loss of operational capability due to earthquakes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested service continuity plan. Such a plan is critical for helping to ensure that information system operations and data can be promptly restored in the event of a disaster. We reported that VA had not completed or tested service continuity plans for several systems. For example, in 1998 we reported that one VA data center had 17 individual disaster recovery plans covering various segments of the organization, but it did not have an overall document that integrated the 17 separate plans and defined the roles and responsibilities for the disaster recovery teams. In 2000, we determined that the service continuity plans for two of the three health care systems we visited did not include critical elements such as detailed recovery procedures, provisions for restoring mission-critical systems, and a list of key contacts; in addition, none of the health care systems we visited were fully testing their service continuity plans.

These deficiencies existed, in part, because VA had not implemented key components of a comprehensive computer security program. Specifically, VA's computer security efforts lacked

- clearly delineated security roles and responsibilities;
- regular, periodic assessments of risk;
- security policies and procedures that addressed all aspects of VA's interconnected environment;
- an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and
- a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

As a result, we made a number of recommendations in 2002 that were aimed at improving VA's security management.²⁰ Among the primary elements of these recommendations were that (1) VA centralize its security management functions and (2) it perform other actions to establish an information security program, including actions related to risk assessments, security policies and procedures, security awareness, and monitoring and evaluating computer controls.²¹

VA's Efforts to Address Information Security Weaknesses Have Been Limited

The department has taken steps to address the weaknesses that we described, but these have not been sufficient to fully implement a comprehensive information security program.²² Examples of actions that VA has taken and still needs to take include the following:

- *Central security management function:* The department realigned its information technology resources to place administration and field office security functions more directly under the oversight of the department's CIO, consolidating all administration-level cyber security functions under the department's cyber security office. In addition, to provide greater management accountability for information security, the Secretary instituted information security standards for members of the department's senior executive service. The cyber security officer organized his office to focus more directly on critical elements of information security control, and he updated the department's security management plan and information

²⁰ GAO, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, [GAO-02-703](#) (Washington, D.C.: June 12, 2002).

²¹ We based our recommendations on guidance and practices provided in GAO, *Federal Information System Controls Audit Manual*, [GAO/AIMD-12.19.6](#) (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, [GAO/AIMD-98-68](#) (Washington, D.C.: May 1998); *Information Security Risk Assessment: Practices of Leading Organizations*, [GAO/AIMD-00-33](#) (Washington, D.C.: November 1999); and Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000). FISMA (passed in late 2002) and associated guidance are generally consistent with this earlier guidance.

²² This result is also reflected in the department's failing grade in the annual report card on computer security that is issued by the House Government Reform Committee: *Computer Security Report Card* (Washington, D.C.: Mar. 16, 2006).

security policies and procedures. However, the department still needed to develop policy and guidance to ensure (1) authority and independence for security officers and (2) departmentwide coordination of security functions.

- *Periodic risk assessments:* VA is implementing a commercial tool to identify the level of risk associated with system changes and also to conduct information security risk assessments. It also created a methodology that establishes minimum requirements for such risk assessments. However, it has not yet completed its risk assessment policy and guidance. VA reported that such guidance was forthcoming as part of an overarching information system security certification and accreditation policy that was to be developed during 2006. Without these elements, VA cannot be assured that it is appropriately performing risk assessments departmentwide.
- *Security policies and procedures:* VA's cyber security officer reported that VA has action ongoing to develop a process for collecting and tracking performance data, ensuring management action when needed, and providing independent validation of reported issues. VA also has ongoing efforts in the area of detecting, reporting, and responding to security incidents. For example, it established network intrusion prevention capability at its four enterprise gateways. It is also developing strategic and tactical plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. However, these plans are not complete.
- *Security awareness:* VA has taken steps to improve security awareness training. It holds an annual department information security conference, and it has developed a Web portal for security training, policy, and procedures, as well as a security awareness course that VA employees are required to review annually. However, VA has not demonstrated that it has a process to ensure compliance.
- *Monitoring and evaluating computer controls:* VA established a process to better monitor and evaluate computer controls by tracking the status of security weaknesses, corrective actions taken, and independent validations of corrective actions through a software data base.²³ However, more remains to be done in this area.

²³ VA's Security Management and Reporting Tool (SMART).

For example, although certain components of VA reported vulnerability and penetration testing to evaluate controls on internal and external access to VA systems, this testing was not part of an ongoing departmentwide program.

Since our last report in 2002, VA's IG and independent auditors have continued to report serious weaknesses with the department's information security controls. The auditors' report on internal controls,²⁴ prepared at the completion of VA's 2005 financial statement audit, identified weaknesses related to access control, segregation of duties, change control, and service continuity—a list of weaknesses that are virtually identical to those we identified years earlier. The department's *FY 2005 Annual Performance and Accountability Report* states that the IG determined that many information system security vulnerabilities reported in national audits from 2001 through 2004 remain unresolved, despite the department's actions to implement IG recommendations in previous audits. The IG also reported specific security weaknesses and vulnerabilities at 45 of 60 VA health care facilities and 11 of 21 VA regional offices where security issues were reviewed, placing VA at risk that sensitive data may be exposed to unauthorized access and improper disclosure, among other things. As a result, the IG determined that weaknesses in VA's information technology security controls were a material weakness.

In response to the IG's findings, the department indicates that plans are being implemented to address the material weakness in information security. According to the department, it has maximized limited resources to make significant improvement in its overall security posture in the near term by prioritizing FISMA remediation activities, and work will continue in the next fiscal year.

Despite these actions, the department has not fully implemented the key elements of a comprehensive security management program, and its efforts have not been sufficient to effectively protect its information systems and information, including personally

²⁴ The auditor's report is included in VA's *FY 2005 Annual Performance and Accountability Report*.

identifiable information, from unauthorized disclosure, misuse, or loss.

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

In addition to establishing a robust information security program, agencies can take other actions to help guard against the possibility that personal information they maintain is inadvertently compromised. These include conducting privacy impact assessments and taking other practical measures.

Conduct Privacy Impact Assessments

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 privacy impact assessments (PIAs), which, as previously mentioned, are required by the E-Government Act of 2002 when agencies use information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider the 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 conduct PIAs as they are required. For example, our review of selected data mining efforts at federal agencies²⁵ 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,²⁶ few PIAs were being developed for systems or programs

²⁵ 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).

²⁶ [GAO-06-421](#), pp. 59–61.

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.

Employ Measures to Prevent Inadvertent Data Breaches

Besides strategic approaches such as establishing an information security program and conducting PIAs, agencies can consider a range of specific practical measures for protecting the privacy and security of personal information. 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 requirements 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.²⁷ As part of their PIAs, federal agencies can make decisions up front about how long they plan to retain personal data, 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 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 need to be stored on portable devices. In certain instances, agencies may find it necessary to enable employees to have access to personal data on portable 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 to gain access to the data. Although encrypting data adds to the operational burden on authorized individuals, who must enter pass codes or use other authentication means to convert the data into readable text, 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 VA. A decision about whether to use encryption would logically be made as an

²⁷ State of California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information* (April 2006), p. 6.

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

In the event a data breach does occur, agencies must respond quickly in order to minimize the potential harm associated with identity theft. 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.²⁸ The Federal Trade Commission has also 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.²⁹

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, California's data breach notification law is credited with bringing to the public's notice large data breaches within the private sector, such as those involving ChoicePoint and LexisNexis last year. 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

²⁸ 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.

²⁹ Synovate, *Federal Trade Commission Identity Theft Survey Report* (McLean, Va.: September 2003).

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.

Breach notification is also important in that it can help an organization address key privacy rights of individuals, in accordance with the fair information practices mentioned earlier. Breach notification is one way that organizations—either in the private sector or the government—can follow the *openness* principle and meet their responsibility for keeping the public informed of how their personal information is being used and who has access to it. Equally important, notification is consistent with the principle that those controlling the collection or use of personal information 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 Commission³⁰ raised concerns about the threshold at 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

³⁰ Federal Trade Commission, *Prepared Statement on Data Breaches and Identity Theft*, p. 10.

not insignificant and may be worth considering. 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 too weak would give companies an incentive not to disclose potentially harmful breaches, and the same concern would 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.³¹ 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.

³¹ Center for Democracy and Technology, *Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Government Use* (Washington, D.C.: Apr. 13, 2005), p. 7.

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.

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.³² 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

³² State of California, *Recommended Practices on Notice of Security Breach*.

-
- 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 it 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 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.³³

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.

³³ Federal Trade Commission, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* (Washington, D.C.: June 2004).

When providing notifications to the public, organizations should consider how to ensure that these are easily understood. Various techniques have been suggested to promote comprehension, including the concept of “layering.”³⁴ Layering involves providing only the most important summary facts up front—often in a graphical format—followed by one or more lengthier, more narrative versions in order to ensure that all information is communicated that needs to be. Multilayering may be an option to achieving an easy-to-understand notice that is still complete. Similarly, providing context to the notice (explaining to consumers why they are receiving the notice and what to do with it) has been found to promote comprehension,³⁵ as did visual design elements such as a tabular format, large and legible fonts, appropriate white space, and simple headings.

Although these techniques were developed for other kinds of notices, they can be applied to those informing the public of data breaches. 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.

³⁴ This concept was discussed during a recent public workshop on “Transparency and Accountability: The Use of Personal Information within the Government,” hosted by the DHS Privacy Office.

³⁵ At the DHS workshop, panelists from the Federal Trade Commission and the Office of the Comptroller of the Currency presented these findings of an interagency research project on design of easy-to-understand consumer financial privacy notices. Kleimann Communication Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006).

In summary, the recent security breach at VA has highlighted the importance of implementing effective information security practices. Long-standing information security control weaknesses at VA have placed its information systems and information, including personally identifiable information, at increased risk of misuse and unauthorized disclosure. Although VA has taken steps to mitigate previously reported weaknesses, it has not implemented a comprehensive, integrated information security program, which it needs in order to effectively manage risks on an ongoing basis. Much work remains to be done. Only through strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight can VA address its persistent, long-standing control weaknesses.

To reduce the likelihood of experiencing such breaches, agencies can take a number of actions that can help guard against the possibility that databases of personally identifiable information are inadvertently compromised: strategically, they should ensure that a robust information security program is in place and that PIAs are developed. 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.

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.

We have previously testified that 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 the public.

Mr. Chairman, this concludes our testimony today. We would be happy to answer any questions you or other members of the committee may have.

Contacts and Acknowledgments

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, koontzl@gao.gov, or Gregory Wilshusen, Director, Information Security, at (202) 512-6244, wilshuseng@gao.gov. Other individuals who made key contributions include Idris Adjerid, Barbara Collier, William Cook, John de Ferrari, Valerie Hopkins, Suzanne Lightman, Barbara Oliver, David Plocher, Jamie Pressman, J. Michael Resser, and Charles Vrael.

Attachment 1: Selected GAO Products

Products Related to VA Information Security

Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure. [GAO/AIMD-98-175](#). Washington, D.C.: September 23, 1998.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. [GAO/AIMD-99-161](#). Washington, D.C.: June 8, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. [GAO/AIMD-00-5](#). Washington, D.C.: October 4, 1999.

VA Systems Security: Information System Controls at the North Texas Health Care System. [GAO/AIMD-00-52R](#). Washington, D.C.: February 1, 2000.

VA Systems Security: Information System Controls at the New Mexico VA Health Care System. [GAO/AIMD-00-88R](#). Washington, D.C.: March 24, 2000.

VA Systems Security: Information System Controls at the VA Maryland Health Care System. [GAO/AIMD-00-117R](#). Washington, D.C.: April 19, 2000.

Information Technology: Update on VA Actions to Implement Critical Reforms. [GAO/T-AIMD-00-74](#). Washington, D.C.: May 11, 2000.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. [GAO/AIMD-00-232](#). Washington, D.C.: September 8, 2000.

Major Management Challenges and Program Risks: Department of Veterans Affairs. [GAO-01-255](#). Washington, D.C.: January 2001.

VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist. [GAO-01-550T](#). Washington, D.C.: April 4, 2001.

VA Information Technology: Progress Made, but Continued Management Attention is Key to Achieving Results. [GAO-02-369T](#). Washington, D.C.: March 13, 2002.

Veterans Affairs: Subcommittee Post-Hearing Questions Concerning the Department's Management of Information Technology. [GAO-02-561R](#). Washington, D.C.: April 5, 2002.

Veterans Affairs: Sustained Management Attention is Key to Achieving Information Technology Results. [GAO-02-703](#). Washington, D.C.: June 12, 2002.

VA Information Technology: Management Making Important Progress in Addressing Key Challenges. [GAO-02-1054T](#). Washington, D.C.: September 26, 2002.

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

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.

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

Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure

Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public. [GAO-05-864R](#). Washington, D.C.: July 22, 2005.

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

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. Chronology of Information Security Weaknesses Identified by GAO

Year	GAO report	VA location or agency	Information security control areas					Security program
			Access control	Physical security	Segregation of duties	Change control	Service continuity	
1998	GAO/AIMD-98-175	Austin	●	●	●	●	●	●
		Dallas	●	●			●	●
		Albuquerque	●	●	●		●	●
		Hines	●					●
		Philadelphia	●					●
1999	GAO/AIMD-99-161	Austin	●			●		●
2000	GAO/AIMD-00-232	Maryland	●	●	●	●	●	●
		New Mexico	●	●	●	●	●	●
		North Texas/Dallas	●	●	●		●	●
2000	GAO/AIMD-00-5	VA	●		●			●
2002	GAO-02-703	VA						●
2005	GAO-05-552	VA	●		●	●	●	●

 Weakness found in this area
 Control area not included in scope of audit

Source: GAO reports.

Notes: Hines is a suburb of Chicago.

Full citations are provided in attachment 1.

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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