United States Government Accountability Office

Testimony
Before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate and the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, November 17, 2015

INFORMATION SECURITY

Federal Agencies Need to Better Protect Sensitive Data

Statement of Joel C. Willemssen,
Managing Director, Information Technology

Accessible Version

GAO Highlights

Highlights of GAO-16-194T, a testimony before the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, U.S. Senate and the Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives

Why GAO Did This Study

Effective information security for federal computer systems and databases is essential to preventing the loss of resources; the unauthorized or inappropriate use, disclosure, or alteration of sensitive information; and the disruption of government operations. Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation’s critical infrastructure. Earlier this year, in GAO’s high-risk update, the area was further expanded to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

This statement summarizes threats and information security weaknesses in federal systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

Over the past 6 years, GAO has made about 2,000 recommendations to improve information security programs and associated security controls. Agencies have implemented about 58 percent of these recommendations. Further, agency inspectors general have made a multitude of recommendations to assist their agencies.

View GAO-16-194T. For more information, contact Joel C. Willemssen at (202) 512-6253 or willemssenj@gao.gov.

November 17, 2015

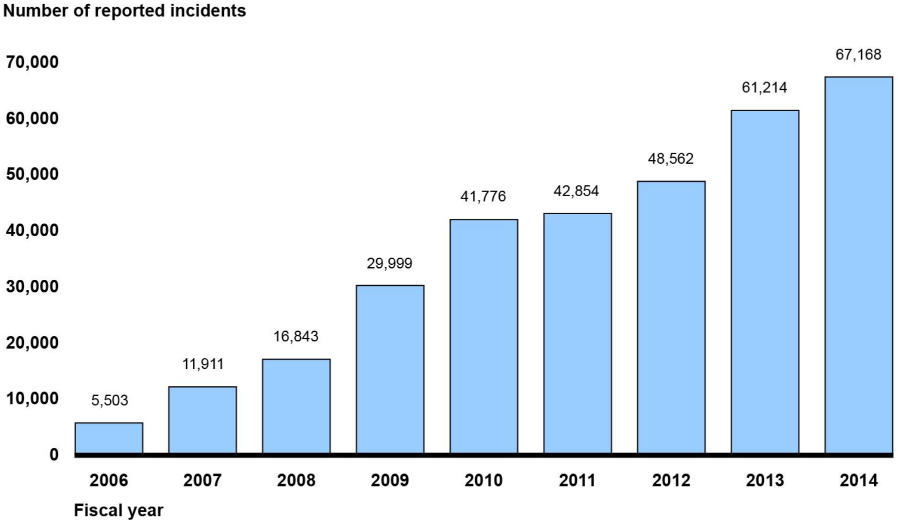
INFORMATION SECURITY

Federal Agencies Need to Better Protect Sensitive Data

What GAO Found

Federal systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from software coding errors or the actions of careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, terrorists, disgruntled employees or other organizational insiders, among others. These concerns are further highlighted by recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years, which have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 (see figure).

Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-16-194T

Data Table for Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

Fiscal Year	Number of Reported Incidents
2006	**5503**
2007	11911
2008	16843
2009	29999
2010	41776
2011	42854
2012	48562
2013	61214
2014	67168

United States Government Accountability Office

Security control weaknesses place sensitive data at risk. GAO has identified a number of deficiencies at federal agencies that pose threats to their information and systems. For example, agencies, including the Department of Homeland Security, have weaknesses with the design and implementation of information security controls, as illustrated by 19 of 24 agencies covered by the *Chief Financial Officers Act* declaring cybersecurity as a significant deficiency or material weakness for fiscal year 2014. In addition, most of the 24 agencies continue to have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware.

Until federal agencies take actions to address these weaknesses—including implementing the thousands of recommendations GAO and agency inspectors general have made—federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats.

Chairman Lankford, Chairman Perry, Ranking Members Heitkamp and Watson Coleman, and Members of the Subcommittees:

Thank you for inviting me to testify at today's hearing on ongoing challenges at the U.S. Secret Service and their government-wide implications. As requested, my statement today will address cyber threats and security control weaknesses affecting federal systems and information.

As you know, the federal government faces an evolving array of cyber-based threats to its systems and data, as illustrated by recently reported data breaches at federal agencies, which have affected millions of current and former federal employees, and the increasing number of incidents reported by agencies. Such incidents underscore the urgent need for effective implementation of information security controls at federal agencies.

Since 1997, we have designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the February 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)[1]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[2]

In preparing this statement, we relied on our previous work addressing cyber threats and federal information security efforts. The prior reports cited throughout this statement contain detailed discussions of the scope of the work and the methodology used to carry it out. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

[1] Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

[2] See GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A list of related GAO products is provided in attachment I.

Background

As computer technology has advanced, the federal government has become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Federal agencies rely on computer systems to transmit proprietary and other sensitive information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services.

Ineffective protection of these information systems and networks can impair delivery of vital services, and result in

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as personally identifiable information;
- disruption of essential operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public’s confidence in government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, Congress enacted laws intended to improve the protection of federal information and systems. These laws include the *Federal Information Security Modernization Act of*

2014 (FISMA),[3] which, among other things, authorizes the Department of Homeland Security (DHS) to (1) assist the Office of Management and Budget (OMB) with overseeing and monitoring agencies' implementation of security requirements; (2) operate the federal information security incident center; and (3) provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities. The act also reiterated the 2002 FISMA requirement for the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems.

In addition, the act continues the requirement for federal agencies to develop, document, and implement an agency-wide information security program. The program is 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.

Cyber Threats to Federal Systems Continue to Evolve Amid Increasing Numbers of Incidents

Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees and other organizational insiders, foreign nations engaged in espionage and information warfare, and terrorists.

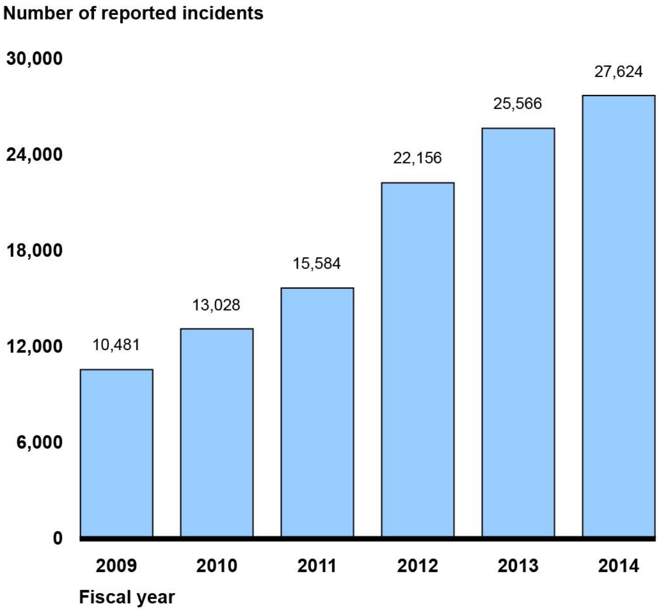
These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary or personal gain or pursuing a political, economic, or military advantage. For example, organizational insiders can pose threats to an organization since their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system, steal system data, or disclose sensitive information without authorization. The insider threat

[3] *The Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) (2014 FISMA) largely superseded the very similar *Federal Information Security Management Act of 2002* (Title III, Pub. L. No. 107-347, Dec. 17, 2002) (2002 FISMA).

includes inappropriate actions by contractors hired by the organization, as well as careless or poorly trained employees.

As we reported in February 2015,[4] since fiscal year 2006, the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent. Furthermore, the number of reported security incidents involving PII at federal agencies has more than doubled in recent years—from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014. (See fig 1.)

Figure 1: Incidents Involving Personally Identifiable Information Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies for Fiscal Years 2009 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2009-2014. | GAO-16-194T

[4] GAO, *High Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

Data Table for Figure 1: Incidents Involving Personally Identifiable Information Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies for Fiscal Years 2009 through 2014

Fiscal Year	Number of reported incidents
2009	10481
2010	13028
2011	15584
2012	22156
2013	25566
2014	27624

These incidents and others like them can adversely affect national security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Recent examples highlight the impact of such incidents:

- In June 2015, the Office of Personnel Management reported that an intrusion into its systems affected the personnel records of about 4.2 million current and former federal employees. The Director stated that a separate but related incident involved the agency's background investigation systems and compromised background investigation files for 21.5 million individuals.
- In June 2015, the Commissioner of the Internal Revenue Service testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to officials, criminals used taxpayer-specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. This data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the agency reported this number to be about 114,000 and that an additional 220,000 accounts had been inappropriately accessed, which brings the total to about 330,000 accounts.
- In April 2015, the Department of Veterans Affairs' Office of Inspector General reported that two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.[5]

[5] Department of Veterans Affairs, Office of Inspector General, *Administrative Investigation Improper Access to the VA Network by VA Contractors from Foreign Countries Office of Information and Technology Austin, TX*, Report No. 13-01730-159 (Washington, D.C.: April 2015).

- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.[6]
- In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.[7]
- In October 2013, a wide-scale cybersecurity breach involving a U.S. Food and Drug Administration system occurred that exposed the PII of 14,000 user accounts.[8]

Information Security Weaknesses Place Federal Systems and Sensitive Data at Risk

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that federal agencies take appropriate steps to secure their systems and information. We and agency inspectors general have identified numerous weaknesses in protecting federal information and systems. Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. Specifically, for fiscal year 2014, 19 of the 24 federal agencies covered by the *Chief Financial Officers Act*[9] reported that information security control deficiencies were either a material weakness or a significant deficiency in

[6] James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Committee on Armed Services, February 26, 2015.

[7] Randy S. Miskanic, Secure Digital Solutions Vice President of the United States Postal Service, *Examining Data Security at the United States Postal Service*, testimony before the Subcommittee on Federal Workforce, U.S. Postal Service and the Census, 113th Congress, November 19, 2014.

[8] Department of Health and Human Services, Office of Inspector General, *Penetration Test of the Food and Drug Administration's Computer Network,* Report No. A-18-13-30331 (Washington, D.C.: October 2014).

[9] The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

internal controls over their financial reporting.[10] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency.

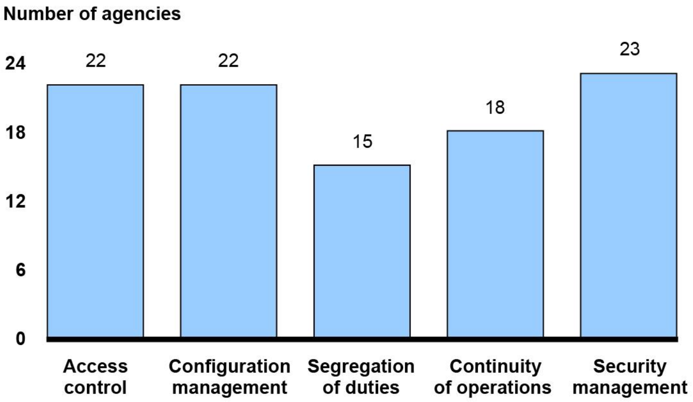
As we reported in September 2015, for fiscal year 2014, most of the 24 agencies had weaknesses in the five major categories of information system controls.[11] These control categories are: (1) access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (2) configuration management controls, intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and assure that software is current and known vulnerabilities are patched; (3) segregation of duties, which prevents a single individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; (4) contingency planning[12], which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide security management, which provides a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended. (See fig. 2.)

[10] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[11] GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015).

[12] Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations.

Figure 2: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-194T

Data Table for Figure 2: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014

Category of weakness	Number of agencies reporting
Access control	22
Configuration management	22
Segregation of duties	12
Continuity of operations	18
Security management	23

- **Access controls:** For fiscal year 2014, we, agencies, and inspectors general reported weaknesses in the electronic and physical controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby increasing their risk of unauthorized use, modification, disclosure, and loss. Access controls involve the six critical elements described in table 1.

Table 1: Critical Elements for Access Control to Computer Resources

Element	Description
Boundary protection	Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices that are connected to a network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection and prevention technologies can be deployed to defend against attacks from the Internet.

Element	Description
User identification and authentication	A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns a unique user account to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication provides the basis for establishing accountability and for controlling access to the system.
Authorization	Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have some built-in authorization features such as permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device. Authorization controls help implement the principle of "least privilege," which the National Institute of Standards and Technology describes as allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Cryptography	Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Examples of cryptographic services are encryption, authentication, digital signature, and key management. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information.
Auditing and Monitoring	To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is necessary to determine what, when, and by whom specific actions have been taken on a system. Agencies do so by implementing software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities.
Physical Security	Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources. Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas is to be managed appropriately.

Source: GAO I GAO-16-194T

For fiscal year 2014, 12 agencies had weaknesses reported in protecting their networks and system boundaries. For example, the access control lists on one agency's firewall did not prevent traffic coming or initiated from the public Internet protocol addresses of a contractor site and a U.S. telecom corporation from entering its network. Additionally, 20 agencies, including DHS, had weaknesses reported in their ability to appropriately identify and authenticate system users. To illustrate, agencies had weak password controls, such as using system passwords that had not been changed from the easily guessable default passwords or did not expire.

Eighteen agencies, including DHS, had weaknesses reported in authorization controls for fiscal year 2014. For example, one agency had not consistently or in a timely manner removed, transferred, and/or terminated employee and contractor access privileges from multiple systems. Another agency also had granted access privileges unnecessarily, which sometimes allowed users of an internal network to read and write files containing sensitive system information. In fiscal year 2014, 4 agencies had weaknesses reported in the use of encryption for protecting data.

In addition, DHS and 18 other agencies had weaknesses reported in implementing an effective audit and monitoring capability. For instance, one agency did not sufficiently log security-relevant events on the servers and network devices of a key system. Moreover, 10 agencies, including DHS, had weaknesses reported in their ability to restrict physical access or harm to computer resources and protect them from unauthorized loss or impairment. For example, a contractor of an agency was granted physical access to a server room without the required approval of the office director.

- **Configuration management:** For fiscal year 2014, 22 agencies, including DHS, had weaknesses reported in controls that are intended to ensure that only authorized and fully tested software is placed in operation, software and hardware is updated, information systems are monitored, patches are applied to these systems to protect against known vulnerabilities, and emergency changes are documented and approved. For example, 17 agencies, including DHS, had weaknesses reported with installing software patches and implementing current versions of software in a timely manner.
- **Segregation of duties:** Fifteen agencies, including DHS, had weaknesses in controls for segregation of duties. These controls are the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a computer-related operation and thereby take unauthorized actions or gain unauthorized access to assets or records. For example, a developer from one agency had been authorized inappropriate access to the production environment of the agency's system.
- **Continuity of operations:** DHS and 17 other agencies had weaknesses reported in controls for their continuity of operations practices for fiscal year 2014. Specifically, 16 agencies did not have a comprehensive contingency plan. For example, one agency's contingency plans had not been updated to reflect changes in the system boundaries, roles and responsibilities, and lessons learned from testing contingency plans at alternate processing and storage

sites. Additionally, 15 agencies had not regularly tested their contingency plans.

- **Security management:** For fiscal year 2014, DHS and 22 other agencies had weaknesses reported in security management, which is an underlying cause for information security weaknesses identified at federal agencies. An agencywide security program, as required by FISMA, provides a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate.

We have also identified inconsistencies with the government's approach to cybersecurity, including the following:

Overseeing the security controls of contractors providing IT services. In August 2014, we reported that five of six agencies we reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls.[13] This was partly because agencies had not documented IT security procedures for effectively overseeing contractor performance. In addition, according to OMB, 16 of 24 agency inspectors general determined that their agency's program for managing contractor systems lacked at least one required element.

Responding to cyber incidents. In April 2014, we reported that the 24 agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[14] Specifically, we estimated that agencies had not completely documented actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[15] In addition, the 6 agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident response activities.

[13] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

[14] GAO*, Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

[15] This estimate was based on a statistical sample of cyber incidents reported in fiscal year 2012, with 95 percent confidence that the estimate falls between 58 and 72 percent.

Responding to breaches of PII. In December 2013, we reported that eight federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.[16] In addition, OMB requirements for reporting PII-related data breaches were not always feasible or necessary. Thus, we concluded that agencies may not be consistently taking actions to limit the risk to individuals from PII-related data breaches and may be expending resources to meet OMB reporting requirements that provide little value.

Over the last several years, we and agency inspectors general have made thousands of recommendations to agencies aimed at improving their implementation of information security controls. For example, we have made about 2,000 recommendations over the last 6 years. These recommendations identify actions for agencies to take in protecting their information and systems. To illustrate, we and inspectors general have made recommendations for agencies to correct weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on their systems. We have also made recommendations for agencies to implement their information security programs and protect the privacy of PII held on their systems.

However, many agencies continue to have weaknesses in implementing these controls in part because many of these recommendations remain unimplemented. For example, about 42 percent of the recommendations we have made during the last 6 years remain unimplemented. Until federal agencies take actions to implement the recommendations made by us and the inspectors general—federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

In conclusion, the dangers posed by a wide array of cyber threats facing the nation are heightened by weaknesses in the federal government's approach to protecting its systems and information. While recent

[16] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

government-wide initiatives, including the 30-day Cybersecurity Sprint,[17] hold promise for bolstering the federal cybersecurity posture, it is important to note that no single technology or set of practices is sufficient to protect against all these threats. A “defense in depth” strategy that includes well-trained personnel, effective and consistently applied processes, and appropriately implemented technologies is required. While agencies have elements of such a strategy in place, more needs to be done to fully implement it and to address existing weaknesses. In particular, implementing our and agency inspectors general recommendations will strengthen agencies’ ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

Chairman Lankford, Chairman Perry, Ranking Members Heitkamp and Watson Coleman, and Members of the Subcommittees, this concludes my statement. I would be happy to answer your questions.

Contact and Acknowledgments

If you have any questions about this statement, please contact Joel C. Willemssen, Managing Director, Information Technology Team, at (202) 512-6253 or willemssenj@gao.gov. Other staff members who contributed to this statement include Gregory C. Wilshusen, Director, Information Security Issues, IT, Larry Crosland (assistant director), Christopher Businsky, Nancy Glover, and Rosanna Guerrero.

[17] In June 2015, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint, during which agencies were to take immediate actions to combat cyber threats within 30 days. Actions included patching critical vulnerabilities, tightening policies and practices for privileged users, and accelerating the implementation of multifactor authentication.

Related GAO Products

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention, GAO-16-174T. Washington, D.C.: October 21, 2015.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity, GAO-16-116T. Washington, D.C.: October 8, 2015.

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs, GAO-15-714. Washington, D.C.: September 29, 2015.

Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies. GAO-15-758T. Washington, D.C.: July 8, 2015.

Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies. GAO-15-725T. Washington, D.C.: June 24, 2015.

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems. GAO-15-573T. Washington, D.C.: April 22, 2015.

Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data. GAO-15-337. Washington, D.C.: March 19, 2015.

Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems. GAO-15-221. Washington, D.C.: January 29, 2015.

Information Security: Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk. GAO-15-220T. Washington, D.C.: November 18, 2014.

Information Security: VA Needs to Address Identified Vulnerabilities. GAO-15-117. Washington, D.C.: November 13, 2014.

Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems. GAO-15-6. Washington, D.C.: December 12, 2014.

Consumer Financial Protection Bureau: Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced. GAO-14-758. Washington, D.C.: September 22, 2014.

Healthcare.Gov: Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses. GAO-14-871T. Washington, D.C.: September 18, 2014.

Healthcare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. GAO-14-730. Washington, D.C.: September 16, 2014.

Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612. Washington, D.C.: August 8, 2014.

Information Security: FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain. GAO-14-674. Washington, D.C.: July 17, 2014.

Information Security: Additional Oversight Needed to Improve Programs at Small Agencies. GAO-14-344. Washington, D.C.: June 25, 2014.

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. GAO-14-459. Washington, D.C.: June 5, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. GAO-14-354. Washington, D.C.: April 30, 2014.

Information Security: SEC Needs to Improve Controls over Financial Systems and Data. GAO-14-419. Washington, D.C.: April 17, 2014.

Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk. GAO-14-405. Washington, D.C.: April 8, 2014.

Information Security: Federal Agencies Need to Enhance Responses to Data Breaches. GAO-14-487T. Washington, D.C.: April 2, 2014.

Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Model. GAO-14-464T. Washington, D.C.: March 26, 2014.

Information Security: VA Needs to Address Long-Standing Challenges. GAO-14-469T. Washington, D.C.: March 25, 2014.

Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. GAO-14-125. Washington, D.C.: January 28, 2014.

Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation. GAO-14-44. Washington, D.C.: January 13, 2014.

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent. GAO-14-34. Washington, D.C.: December 9, 2013.

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. GAO-13-776. Washington, D.C.: September 26, 2013.

Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts. GAO-13-275. Washington, D.C.: April 10, 2013.

Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses. GAO-13-350. Washington, D.C.: March 15, 2013.

Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges. GAO-13-462T. Washington, D.C.: March 7, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2013.

Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project. GAO-13-155. Washington, D.C.: January 25, 2013.

Information Security: Actions Needed by Census Bureau to Address Weaknesses. GAO-13-63. Washington, D.C.: January 22, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO-12-757. Washington, D.C.: September 18, 2012.

Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy. GAO-12-903. Washington, D.C.: September 11, 2012.

Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. GAO-12-816. Washington, D.C.: August 31, 2012.

Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape. GAO-12-961T. Washington, D.C.: July 31, 2012.

Information Security: Environmental Protection Agency Needs to Resolve Weaknesses. GAO-12-696. Washington, D.C.: July 19, 2012.

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

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight. GAO-12-479. Washington, D.C.: July 9, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T. Washington, D.C.: June 28, 2012.

Prescription Drug Data: HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight. GAO-12-605. Washington, D.C.: June 22, 2012.

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

Management Report: Improvements Needed in SEC's Internal Control and Accounting Procedure. GAO-12-424R. Washington, D.C.: April 13, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. Washington, D.C.: March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO-12-393. Washington, D.C.: March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO-12-507T. Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO-12-8. Washington, D.C.: November 29, 2011.

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

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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548