United States Government Accountability Office

Testimony

Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, July 8, 2015

INFORMATION SECURITY

Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

July 8, 2015

INFORMATION SECURITY

Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies

Highlights of GAO-15-758T, a testimony before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives

Why GAO Did This Study

Effective cybersecurity for federal information systems is essential to preventing the loss of resources, the compromise 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 (1) cyber threats to federal systems, (2) challenges facing federal agencies in securing their systems and information, and (3) government-wide initiatives aimed at improving cybersecurity. In preparing this statement, GAO relied on its previously published and ongoing work in this area.

What GAO Recommends

In previous work, GAO and agency inspectors general have made hundreds of recommendations to assist agencies in addressing cybersecurity challenges. GAO has also made recommendations to improve government-wide initiatives.

View GAO-15-758T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure or careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, or terrorists, among others. Threat actors use a variety of attack techniques that can adversely affect federal information, computers, software, networks, or operations, potentially resulting in the disclosure, alteration, or loss of sensitive information; destruction or disruption of critical systems; or damage to economic and national security. 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.

GAO has identified a number of challenges federal agencies face in addressing threats to their cybersecurity. For example, agencies have been challenged with designing and implementing risk-based cybersecurity programs, as illustrated by 19 of 24 major agencies declaring cybersecurity as a significant deficiency or material weakness for financial reporting purposes. Other challenges include:

- enhancing oversight of contractors providing IT services,
- improving security incident response activities,
- responding to breaches of personal information, and
- implementing cybersecurity programs at small agencies.

Until federal agencies take actions to address these challenges—including implementing the hundreds 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.

Several government-wide initiatives are under way to bolster cybersecurity.

- **Personal Identity Verification:** The President and the Office of Management and Budget (OMB) directed agencies to issue credentials with enhanced security features to control access to federal facilities and systems. OMB recently reported that only 41 percent of user accounts at 23 civilian agencies had required these credentials to access agency systems.
- **Continuous Diagnostics and Mitigation:** This program is to provide agencies with tools for continuously monitoring cybersecurity risks. The Department of State adopted a continuous monitoring program, and GAO reported on the benefits and challenges in implementing the program.
- **National Cybersecurity Protection System:** This system is to provide capabilities for monitoring network traffic and detecting and preventing intrusions. GAO has ongoing work reviewing the system's implementation. Preliminary observations indicate that implementation of the intrusion detection and prevention capabilities may be limited and requirements for future capabilities appear to have not been fully defined.

While these initiatives are intended to improve security, no single technology or tool is sufficient to protect against all cyber threats. Rather, agencies need to employ a multi-layered approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.

Chairwoman Comstock, Chairman Loudermilk, Ranking Members Lipinski and Beyer, and Members of the Subcommittees:

Thank you for inviting me to testify at today's hearing on data breaches at the Office of Personnel Management (OPM) and cybersecurity challenges faced by federal agencies. As you know, the federal government faces an array of cyber-based threats to its systems and data, as illustrated by the recently reported data breaches at OPM, which affected millions of current and former federal employees. 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]

My statement today will discuss (1) cyber threats facing federal systems, (2) challenges that federal agencies face in securing their systems and information, and (3) government-wide initiatives aimed at improving agencies' cybersecurity. In preparing this statement, we relied on our previous work in these areas, as well as the preliminary observations from our ongoing review of the Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS) initiative. We discussed these observations with DHS officials. 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 or is being conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[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).

evidence to provide a reasonable basis for our findings and conclusions 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.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations 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. In addition, the Internet has grown increasingly important to American businesses and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, and has developed into an extended information and communications infrastructure that supports vital services such as power distribution, health care, law enforcement, and national defense.

Ineffective protection of these information systems and networks can result in a failure to deliver these 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 national security information, PII, and proprietary business 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 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.

The Federal Government Faces an Evolving Array of Cyber-Based Threats

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, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, 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 gain or a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. Table 1 describes common cyber adversaries.

[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).

Table 1: Common Cyber Adversaries

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers/hacktivists	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to potentially have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his February 2015 testimony, the Director of National Intelligence stated that, among state actors, China, and Russia have highly sophisticated cyber programs, while Iran and North Korea have lesser technical capabilities but possibly more disruptive intent.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center. | GAO-15-758T

These adversaries make use of various techniques— or exploits—that may adversely affect federal information, computers, software, networks, and operations. Table 2 describes common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service/distributed denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Phishing/spear phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Spear phishing is a phishing exploit that is targeted to a specific individual or group.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports; and GAO. | GAO-15-758T

An adversary may employ multiple tactics, techniques, and exploits to conduct a cyber attack. The National Institute of Standards and Technology (NIST) has identified several representative events that may constitute a cyber attack:[4]

[4]NIST, *Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

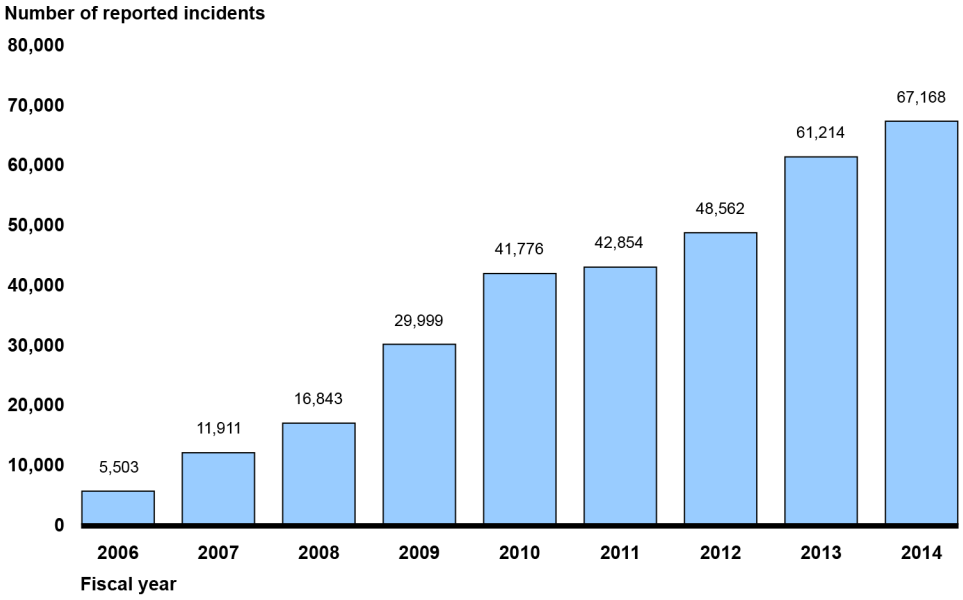
- **Perform reconnaissance and gather information:** An adversary may gather information on a target by, for example, scanning its network perimeters or using publicly available information.
- **Craft or create attack tools:** An adversary prepares its means of attack by, for example, crafting a phishing attack or creating a counterfeit ("spoof") website.
- **Deliver, insert, or install malicious capabilities:** An adversary can use common delivery mechanisms, such as e-mail or downloadable software, to insert or install malware into its target's systems.
- **Exploit and compromise:** An adversary may exploit poorly configured, unauthorized, or otherwise vulnerable information systems to gain access.
- **Conduct an attack:** Attacks can include efforts to intercept information or disrupt operations (e.g., denial of service or physical attacks).
- **Achieve results:** Desired results include obtaining sensitive information via network "sniffing" or exfiltration, causing degradation or destruction of the target's capabilities; damaging the integrity of information through creating, deleting, or modifying data; or causing unauthorized disclosure of sensitive information.
- **Maintain a presence or set of capabilities:** An adversary may try to maintain an undetected presence on its target's systems by inhibiting the effectiveness of intrusion-detection capabilities or adapting behavior in response to the organization's surveillance and security measures.

More generally, the nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attacks do not require physical proximity to their victims, can be carried out at high speeds and directed at multiple victims simultaneously, and can more easily allow attackers to remain anonymous. These inherent advantages, combined with the increasing sophistication of cyber tools and techniques, allow threat actors to target government agencies and their contractors, potentially resulting in the disclosure, alteration, or loss of sensitive information, including PII; theft of intellectual property; destruction or disruption of critical systems; and damage to economic and national security.

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. (See fig. 1.)

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

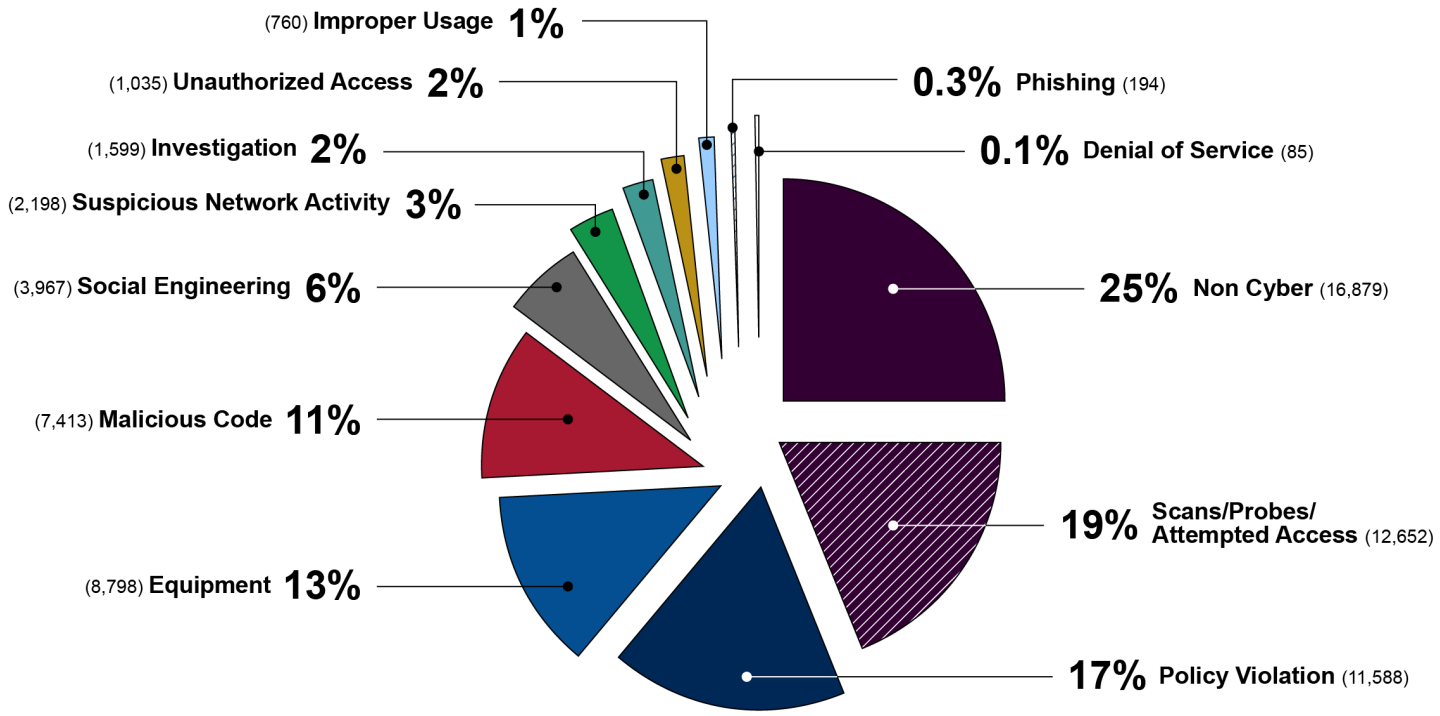


Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-758T

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.

Figure 2 shows the different types of incidents reported in fiscal year 2014.

Figure 2: Information Security Incidents by Category, Fiscal Year 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-758T

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, OPM reported that an intrusion into its systems affected personnel records of about 4 million current and former federal employees. The Director of OPM also stated that a separate incident may have compromised OPM systems related to background investigations, but its scope and impact have not yet been determined.
- In June 2015, the Commissioner of the Internal Revenue Service (IRS) testified that unauthorized third parties had gained access to taxpayer information from its “Get Transcript” application. According to IRS, criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses.

- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally owned equipment.
- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on OPM's networks and those of two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.
- 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.

Federal Agencies Face Ongoing Cybersecurity Challenges

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 challenges in protecting federal information and systems, including those in the following key areas:

- **Designing and implementing risk-based cybersecurity programs at federal agencies.** 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 (CFO) Act[5] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over

[5]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.

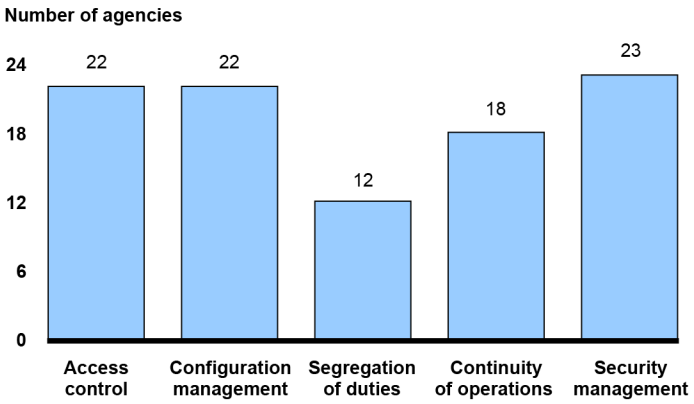
their financial reporting.[6] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency.

As we testified in April 2015, for fiscal year 2014, most of the agencies had weaknesses in the five key security control categories.[7] These control categories are (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis. (See fig. 3.)

[6]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.

[7]GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*, GAO-15-573T (Washington, D.C.: Apr. 22, 2015).

Figure 3: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-758T

Examples of these weaknesses include: (1) granting users access permissions that exceed the level required to perform their legitimate job-related functions; (2) not ensuring that only authorized users can access an agency's systems; (3) not using encryption to protect sensitive data from being intercepted and compromised; (4) not updating software with the current versions and latest security patches to protect against known vulnerabilities; and (5) not ensuring employees were trained commensurate with their responsibilities. We and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of these information security controls.

- **Enhancing oversight 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.[8] 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. We recommended that the reviewed agencies establish and

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

implement IT security oversight procedures for such systems. The agencies generally concurred with our recommendations. We also made one recommendation to OPM and the agency concurred, but has not yet implemented this recommendation.

- **Improving security incident response activities**. In April 2014, we reported that the 24 agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[9] 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.[10] In addition, the 6 agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident response activities. We recommended that OMB address agency incident response practices government-wide and that the 6 agencies improve the effectiveness of their cyber incident response programs. The agencies generally agreed with these recommendations.
- **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.[11] 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. We recommended that OMB revise its guidance to agencies on responding to a PII-related data breach and that the reviewed agencies take specific actions to improve their response to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation; four of the reviewed agencies agreed, two partially agreed, and two neither agreed nor disagreed.
- **Implementing security programs at small agencies.** In June 2014, we reported that six small agencies (i.e., agencies with 6,000 or fewer

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

[10]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.

[11]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).

employees) had not implemented or not fully implemented their information security programs.[12] For example, key elements of their plans, policies, and procedures were outdated, incomplete, or did not exist, and two of the agencies had not developed an information security program with the required elements. We recommended that OMB include a list of agencies that did not report on the implementation of their information security programs in its annual report to Congress on compliance with the requirements of FISMA, and include information on small agencies' programs. OMB generally concurred with our recommendations. We also recommended that DHS develop guidance and services targeted at small agencies. DHS agreed and has implemented this recommendation.

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

Government-wide Cybersecurity Initiatives Present Potential Benefits and Challenges

In addition to the efforts of individual agencies, DHS and OMB have several initiatives under way to enhance cybersecurity across the federal government. While these initiatives all have potential benefits, they also have limitations.

Personal Identity Verification: In August 2004, Homeland Security Presidential Directive 12 ordered the establishment of a mandatory, government-wide standard for secure and reliable forms of identification for federal government employees and contractor personnel who access government-controlled facilities and information systems. Subsequently, NIST defined requirements for such personal identity verification (PIV) credentials based on "smart cards"—plastic cards with integrated circuit chips to store and process data—and OMB directed federal agencies to issue and use PIV credentials to control access to federal facilities and systems.

In September 2011, we reported that OMB and the eight agencies in our review had made mixed progress for using PIV credentials for controlling

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

access to federal facilities and information systems.[13] We attributed this mixed progress to a number of obstacles, including logistical problems in issuing PIV credentials to all agency personnel and agencies not making this effort a priority. We made several recommendations to the eight agencies and to OMB to more fully implement PIV card capabilities. Although two agencies did not comment, seven agencies agreed with our recommendations or discussed actions they were taking to address them. For example, we made four recommendations to DHS. The department concurred and has taken action to implement them.

In February 2015, OMB reported that, as of the end of fiscal year 2014, only 41 percent of agency user accounts at the 23 civilian CFO Act agencies required PIV cards for accessing agency systems.[14] At OPM, only 1 percent of user accounts required PIV cards for such access.

Continuous Diagnostics and Mitigation (CDM): According to DHS, this program is intended to provide federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into a dashboard that alerts network managers. These alerts can be prioritized, enabling agencies to allocate resources based on risk. DHS, in partnership with the General Services Administration, has established a government-wide contract that is intended to allow federal agencies (as well as state, local, and tribal governmental agencies) to acquire CDM tools at discounted rates.

In July 2011, we reported on the Department of State's (State) implementation of its continuous monitoring program, referred to as iPost.[15] We determined that State's implementation of iPost had improved

[13]GAO, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards,* GAO-11-751 (Washington, D.C.: Sept. 20, 2011).

[14]OMB, *Annual Report to Congress: Federal Information Security Management Act* (Washington, D.C.: Feb. 27, 2015).

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

visibility over information security at the department and helped IT administrators identify, monitor, and mitigate information security weaknesses. However, we also noted limitations and challenges with State's approach, including ensuring that its risk-scoring program identified relevant risks and that iPost data were timely, complete, and accurate. We made several recommendations to improve the implementation of the iPost program, and State partially agreed.

National Cybersecurity Protection System (NCPS): The National Cybersecurity Protection System, operationally known as "EINSTEIN," is a suite of capabilities intended to detect and prevent malicious network traffic from entering and exiting federal civilian government networks. The EINSTEIN capabilities of NCPS are described in table 3.[16]

Table 3: National Cybersecurity Protection System EINSTEIN Capabilities

Operational name	Capability intended	Description
EINSTEIN 1	Network Flow	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections.[a]
EINSTEIN 2	Intrusion Detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts US-CERT when specific network activity matching the predetermined signatures is detected.[b]
EINSTEIN 3 Accelerated	Intrusion Prevention	Automatically blocks malicious traffic from entering or leaving federal civilian executive branch agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision-making using DHS-developed indicators of malicious cyber activity to develop signatures.[c]

Source: GAO analysis of DHS documentation and prior GAO reports. | GAO-15-758T

[a]The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[b]Signatures are recognizable, distinguishing patterns associated with cyber attacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

[c]An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to Internet Protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either classified or unclassified.

In March 2010, we reported that while agencies that participated in EINSTEIN 1 improved their identification of incidents and mitigation of attacks, DHS lacked performance measures to understand if the initiative

[16]In addition to the EINSTEIN capabilities listed in table 1, NCPS also includes a set of capabilities related to analytics and information sharing.

was meeting its objectives.[17] We made four recommendations regarding the management of the EINSTEIN program, and DHS has since taken action to address them.

Currently, we are reviewing NCPS as directed by Senate and House reports accompanying the Consolidated Appropriations Act, 2014. The objectives of our review are to determine the extent to which (1) NCPS meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system.

Our final report is expected to be released later this year, and our preliminary observations include the following:

- DHS appears to have developed and deployed aspects of the intrusion detection and intrusion prevention capabilities, but potential weaknesses may limit their ability to detect and prevent computer intrusions. For example, NCPS detects signature anomalies using only one of three detection methodologies identified by NIST: signature-based, anomaly-based, and stateful protocol analysis. Further, the system has the ability to prevent intrusions, but is currently only able to proactively mitigate threats across a limited subset of network traffic (i.e., Domain Name System traffic and e-mail).
- DHS has identified a set of NCPS capabilities that are planned to be implemented in fiscal year 2016, but it does not appear to have developed formalized requirements for capabilities planned through fiscal year 2018.
- The NCPS intrusion detection capability appears to have been implemented at 23 CFO Act agencies.[18] The intrusion prevention capability appears to have limited deployment at portions of only 5 of these agencies. Deployment may have been hampered by various implementation and policy challenges.

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

[17]GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, D.C.: Mar. 12, 2010).

[18]The Department of Defense is not required to implement EINSTEIN.

government-wide initiatives 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 is required that includes well-trained personnel, effective and consistently applied processes, and appropriately implemented technologies. 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 GAO and inspector general recommendations will strengthen agencies’ ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

Chairwoman Comstock, Chairman Loudermilk, Ranking Members Lipinski and Beyer, 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 Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff members who contributed to this statement include Larry Crosland and Michael Gilmore (assistant directors), Bradley Becker, Christopher Businsky, Nancy Glover, Rosanna Guerrero, Kush Malhotra, and Lee McCracken.

Related GAO Products

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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 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. 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

Please Print on Recycled Paper.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.