United States Government Accountability Office

Testimony

Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, April 22, 2015

CYBERSECURITY

Actions Needed to Address Challenges Facing Federal Systems

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

April 22, 2015

CYBERSECURITY

Actions Needed to Address Challenges Facing Federal Systems

Highlights of GAO-15-573T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Federal agencies, as well as their contractors, depend on interconnected computer systems and electronic data to carry out essential mission-related functions. Thus, the security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. If information security controls are ineffective, resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructure could be disrupted, with potentially catastrophic effects. Federal law sets forth various requirements, roles, and responsibilities for securing federal agencies' systems and information. In addition, GAO has designated federal information security as a high-risk area since 1997.

GAO was asked to provide a statement summarizing cyber threats facing federal agency and contractor systems, and challenges in securing these systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

In its previous work, GAO has made numerous recommendations to agencies to assist in addressing the identified cybersecurity challenges.

View GAO-15-573T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal and contractor systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure, 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 the sharp increase in cyber incidents reported by federal agencies over the last several years, as well as the reported impact of such incidents on government and contractor systems.

Because of the risk posed by these threats, it is crucial that the federal government take appropriate steps to secure its information and information systems. However, GAO has identified a number of challenges facing the government's approach to cybersecurity, including the following:

- **Implementing risk-based cybersecurity programs at federal agencies:** For fiscal year 2014, 19 of 24 major federal agencies reported that deficiencies in information security controls constituted either a material weakness or significant deficiency in internal controls over their financial reporting. In addition, inspectors general at 23 of these agencies cited information security as a major management challenge for their agency.
- **Securing building and access control systems:** GAO previously reported that the Department of Homeland Security lacked a strategy for addressing cyber risks to agencies' building and access control systems—computers that monitor and control building operations—and that the General Services Administration had not fully assessed the risk of cyber attacks to such systems.
- **Overseeing contractors:** The agencies GAO reviewed were inconsistent in overseeing contractors' implementation of security controls for systems they operate on behalf of agencies.
- **Improving incident response:** The agencies GAO reviewed did not always effectively respond to cybersecurity incidents or develop comprehensive policies, plans, and procedures to guide incident-response activities.
- **Responding to breaches of personally identifiable information:** The agencies GAO reviewed have inconsistently implemented policies and procedures for responding to data breaches involving sensitive personal information.
- **Implementing security programs at small agencies:** Smaller federal agencies (generally those with 6,000 or fewer employees) have not always fully implemented comprehensive agency-wide information security programs.

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

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for inviting me to testify about cyber threats facing federal information systems at today's hearing. As you know, federal agencies and their contractors are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern. In February 2015, the Director of National Intelligence testified that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.[1]

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

As discussed with your staff, my testimony today will describe (1) cyber threats facing federal and contractor systems and (2) challenges in securing them, as well as actions needed to address these challenges. In preparing this statement in April 2015 we relied on our previous work in these areas.[3] The reports presenting this work contain detailed overviews of its scope and the methodology we used to carry it out. 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]James R. Clapper, Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Armed Services Committee (February 26, 2015).

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

[3]See the list of related GAO products at the end of this statement.

based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

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 sensitive and proprietary 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 business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, as well as developing into an extended information and communications infrastructure supporting vital services such as power distribution, health care, law enforcement, and national defense.

Consequently, the security of these systems and networks is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including

- 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, personally identifiable information (PII),[4] or proprietary business information;
- disruption of critical 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.

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

Recognizing the importance of these issues, Congress recently enacted laws intended to improve federal cybersecurity. These include the Federal Information Security Modernization Act of 2014 (FISMA), which revised the Federal Information Security Management Act of 2002 to, among other things, clarify and strengthen information security roles and responsibilities for the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The act also reiterated 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.

In addition, the Cybersecurity Workforce Assessment Act and the Homeland Security Cybersecurity Workforce Assessment Act aim to help DHS address its cybersecurity workforce challenges. Another law, the National Cybersecurity Protection Act of 2014, codifies the role of DHS's National Cybersecurity and Communications Integration Center as the federal civilian interface for sharing information between federal and nonfederal entities regarding cyber risk, incidents, analysis, and warnings. The Cybersecurity Enhancement Act of 2014, among other things, authorizes the National Institute of Standards and Technology (NIST) to facilitate and support the development of voluntary standards to reduce cyber risks to critical infrastructure and to develop and encourage the implementation of a strategy for the use and adoption of cloud computing services by the federal government.

The Federal Government and Its Contractors Face an Evolving Array of Cyber-Based Threats

Risks to cyber-based assets can originate from unintentional and intentional threats. Unintentional threats can be caused by, among other things, 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.

Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. 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 sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

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-15-573T

These threat sources 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-15-573T

An adversarial threat source may employ multiple tactics, techniques, and exploits to conduct a cyber attack. NIST has identified several representative events that may constitute a cyber attack:[5]

- **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.

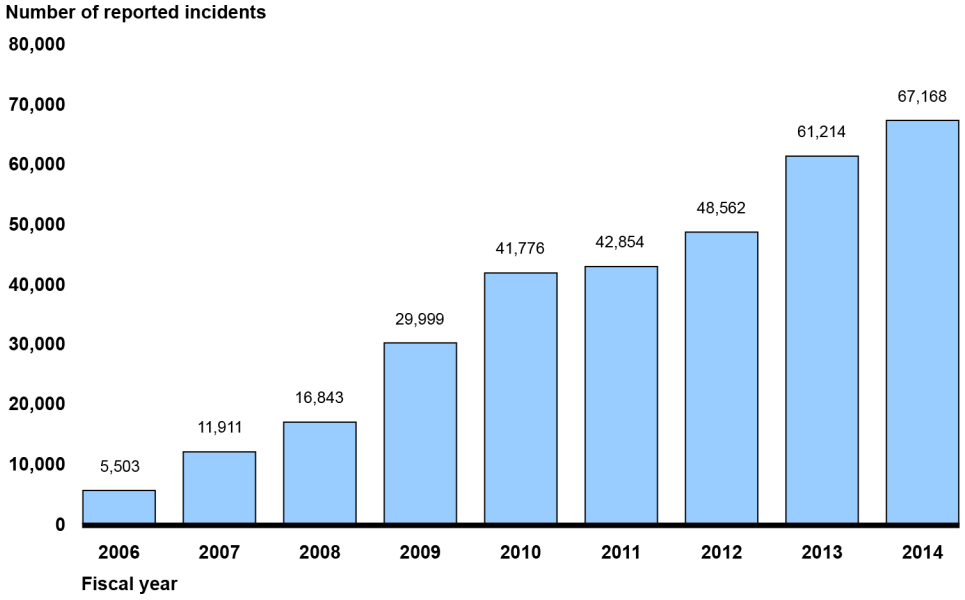
More generally, the nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attacks do not require physical proximity to their victims, can be carried out at high speeds and directed at multiple victims simultaneously, and can more easily allow attackers to remain 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

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

disruption of critical systems; and damage to economic and national security.

The number of information security incidents affecting systems supporting the federal government is increasing. Specifically, the number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) increased 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

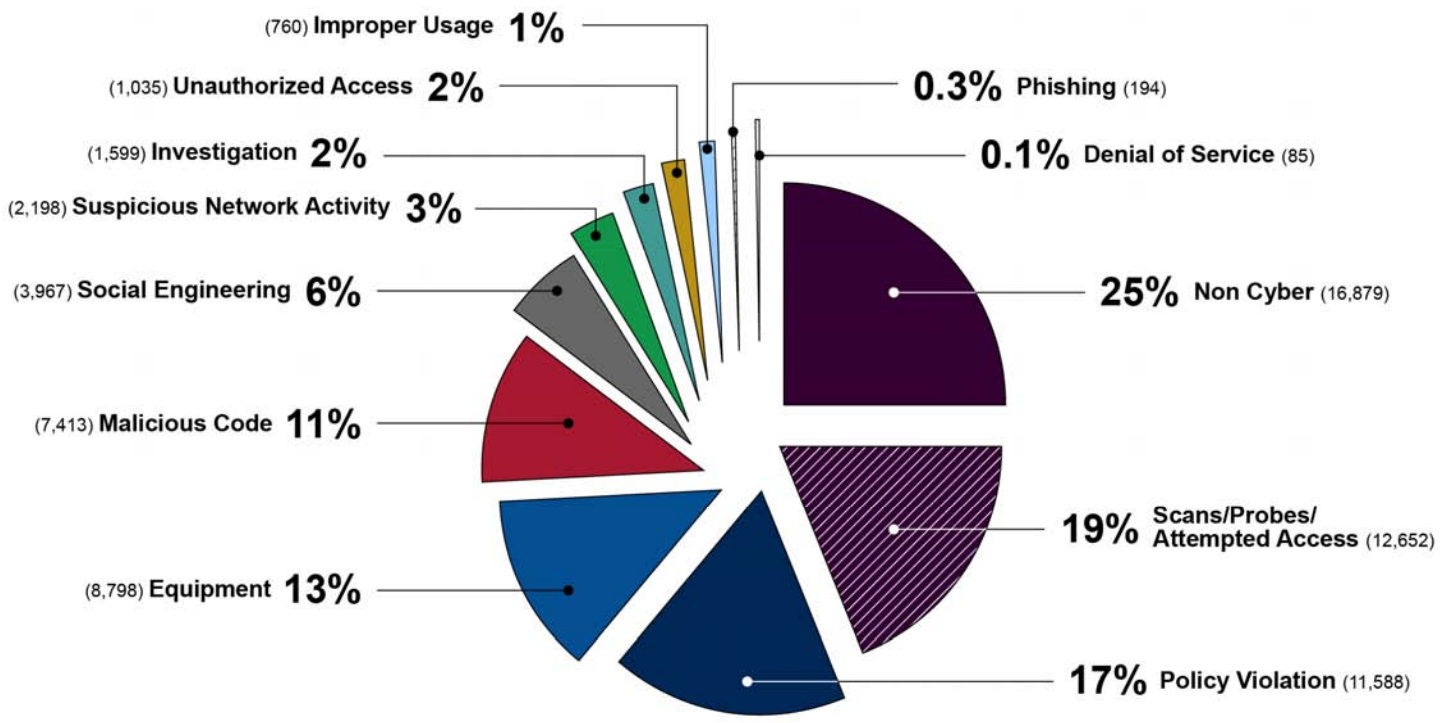


Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-573T

Similarly, the number of information security incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 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-15-573T

These incidents and others like them could 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 potential impact of such incidents:

- 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 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.
- According to the Director of National Intelligence, 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.
- In 2011, according to a media report, the Deputy Secretary of Defense acknowledged a significant cyber attack in which a large number of files was taken by foreign intruders from a defense contractor. The deputy secretary was quoted as saying "it is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies" and that some of the data concerned "our most sensitive systems."

The Federal Government Faces Ongoing Challenges in Its Approach to Cybersecurity

Given the risk posed by cyber threats and the increasing number of incidents, it is crucial that the federal government take appropriate steps to secure its systems and information. However, both we and agency inspectors general have identified challenges in the government's approach to cybersecurity, including those related to protecting the government's information and systems. In particular, challenges remain 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

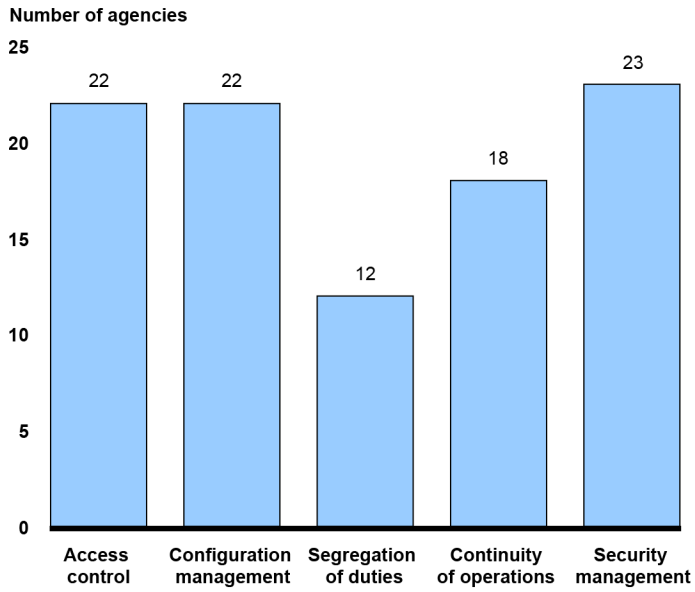
monitoring results. Specifically, for fiscal year 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers Act[6] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting.[7] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency. For fiscal year 2014, most of the agencies had weaknesses in five key security control categories.[8] Figure 3 shows the number of the 24 agencies reviewed with weaknesses in each of the five control categories for fiscal year 2014.

[6]The 24 CFO Act 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.

[7]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.

[8]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 information security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks regularly.

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



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-573T

Over the last several years, GAO and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of information security controls. For example:

- **Addressing cybersecurity for building and access control systems.** In December 2014 we reported that DHS lacked a strategy for addressing cyber risk to building and access control systems[9] and that its Interagency Security Committee had not included cyber threats to such systems in its threat report to federal agencies.[10] Further, the General Services Administration (GSA) had not fully assessed the risk of cyber attacks aimed at building control systems. We recommended that DHS and GSA take steps to address these weaknesses. DHS and GSA agreed with our recommendations.

[9]Building and access control systems are computers that monitor and control building operations such as elevators; electrical power; and heating, ventilation, and air conditioning.

[10]GAO, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, GAO-15-6 (Washington, D.C.: Dec. 12, 2014).

- **Enhancing oversight of contractors providing IT services.** In August 2014 we reported that five of six agencies reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls.[11] 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 found that their agency's program for managing contractor systems lacked at least one required element. We recommended that OMB, in conjunction with DHS, develop and clarify guidance to agencies for annually reporting the number of contractor-operated systems and that the reviewed agencies establish and implement IT security oversight procedures for such systems. OMB did not comment on our report, but the agencies generally concurred with our recommendations.
- **Improving security incident response activities.** In April 2014 we reported that the 24 major agencies did not consistently demonstrate that they had been effectively responding to cyber incidents.[12] Specifically, we estimated that agencies did not completely document actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[13] In addition, six agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident-response activities. We recommended that DHS and OMB address agency incident-response practices government-wide and that the six agencies in our review 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.[14] 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

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

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

[13]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.

[14]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).

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 on federal agencies' responses 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 employees) had not fully implemented their information security programs.[15] 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, as well as including information on small agencies' programs. We also recommended that DHS develop guidance and services targeted at small agencies. OMB and DHS generally concurred with our recommendations.

Until federal agencies take actions to address these challenges—including implementing the hundreds of recommendations made by us and inspectors general—federal systems and information, as well as sensitive personal information about members of the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

In summary, the cyber threats facing the nation are evolving and growing, with a wide array of threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by weaknesses in the federal government's approach to protecting federal systems and information, including personally identifiable information entrusted to the government by members of the public. Implementing GAO's many outstanding recommendations will assist agencies in better protecting their systems and information, which will in turn reduce the risk of the potentially devastating impacts of cyber attacks.

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

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Larry Crosland (Assistant Director), Rosanna Guerrero, Fatima Jahan, and Lee McCracken.

Related GAO Products

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: Privacy and Security Controls for Data Collections Should Be 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.

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

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.