United States Government Accountability Office

Testimony Before the President's Commission on Enhancing National Cybersecurity

For Release on Delivery
September 19, 2016

FEDERAL INFORMATION SECURITY

Actions Needed to Address Challenges

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

Accessible Version

GAO-16-885T

GAO Highlights

Highlights of GAO-16-885T, a testimony before the President's Commission on Enhancing National Cybersecurity

September 19, 2016

FEDERAL INFORMATION SECURITY

Actions Needed to Address Challenges

Why GAO Did This Study

The dependence of federal agencies on computerized information systems and electronic data makes them potentially vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's safety, prosperity, and well-being.

Because of the significance of these risks and long-standing challenges in effectively implementing information security protections, GAO has designated federal information security as a government-wide high-risk area since 1997. In 2003 this area was expanded to include computerized systems supporting the nation's critical infrastructure, and again in February 2015 to include protecting the privacy of personally identifiable information collected, maintained, and shared by both federal and nonfederal entities.

GAO was asked to provide a statement on laws and policies shaping the federal IT security landscape and actions needed for addressing long-standing challenges to improving the nation's cybersecurity posture. In preparing this statement, GAO relied on previously published work.

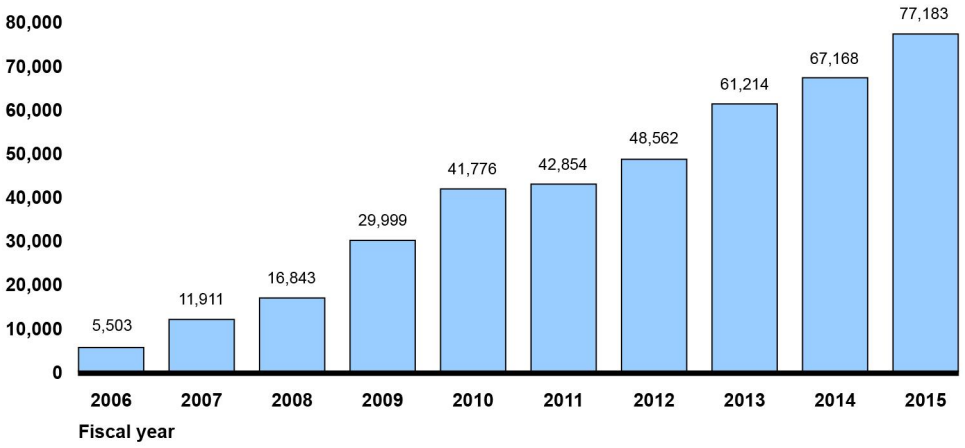
Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of September 16, 2016, about 1,000 have not been implemented.

View GAO-16-885T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cyber incidents affecting federal agencies have continued to grow, increasing about 1,300 percent from fiscal year 2006 to fiscal year 2015.

Cyber Incidents Reported by Federal Agencies, Fiscal Year 2006--2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Several laws and policies establish a framework for the federal government's information security and assign implementation and oversight responsibilities to key federal entities, including the Office of Management and Budget, executive branch agencies, and the Department of Homeland Security (DHS).

However, implementation of this framework has been inconsistent, and additional actions are needed:

- **Effectively implement risk-based information security programs.** Agencies have been challenged to fully and effectively establish and implement information security programs. They need to enhance capabilities to identify cyber threats, implement sustainable processes for securely configuring their computer assets, patch vulnerable systems and replace unsupported software, ensure comprehensive testing and evaluation of their security on a regular basis, and strengthen oversight of IT contractors.
- **Improve capabilities for detecting, responding to, and mitigating cyber incidents.** Even with strong security, organizations can continue to be victimized by attacks exploiting previously unknown vulnerabilities. To address this, DHS needs to expand the capabilities and adoption of its intrusion detection and prevention system, and agencies need to improve their practices for responding to cyber incidents and data breaches.
- **Expand cyber workforce and training efforts.** Ensuring that the government has a sufficient cybersecurity workforce with the right skills and training remains an ongoing challenge. Government-wide efforts are needed to better recruit and retain a qualified cybersecurity workforce and to improve workforce planning activities at agencies.

Chairman Donilon, Vice Chair Palmisano, and distinguished members of the Commission, thank you for the opportunity to appear before you today to discuss laws and policies shaping the federal government's information technology (IT) security landscape and the actions needed to address long-standing challenges to improving the government's cybersecurity posture.

My name is Greg Wilshusen and I serve as the Director of Information Security Issues for the U.S. Government Accountability Office (GAO). GAO is an independent agency in the legislative branch of the federal government. Our mission is to help Congress improve the performance and accountability of the federal government for the benefit of the American people. In other words, we examine how taxpayer dollars are spent and advise lawmakers and agency heads on ways to make government work better. In my position, I am responsible for leading audits and studies of the security of federal information systems and cyber critical infrastructure and the privacy of personally identifiable information. My statement today is based on our previously published work addressing federal cybersecurity efforts.[1]

As computer technology has advanced, federal agencies have become dependent on computerized 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. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective controls can result in significant risk to a broad array of government operations and assets. For example:

- Resources, such as payments and collections, could be lost or stolen.

[1]The reports cited in this statement contain detailed discussions of the scope of the work and the methodology used to carry it out. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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.

- Computer resources could be used for unauthorized purposes, including launching attacks on others.
- Sensitive information, such as intellectual property and national security data, and personally identifiable information, such as taxpayer data, Social Security records, and medical records, could be inappropriately added to, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud or disruption.
- Entity missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by the Mitre Corporation has identified 78,907 publicly known cybersecurity vulnerabilities and exposures as of September 15, 2016, with more being added each day.[2] Federal systems and networks are also often interconnected with other internal and external systems and networks, including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

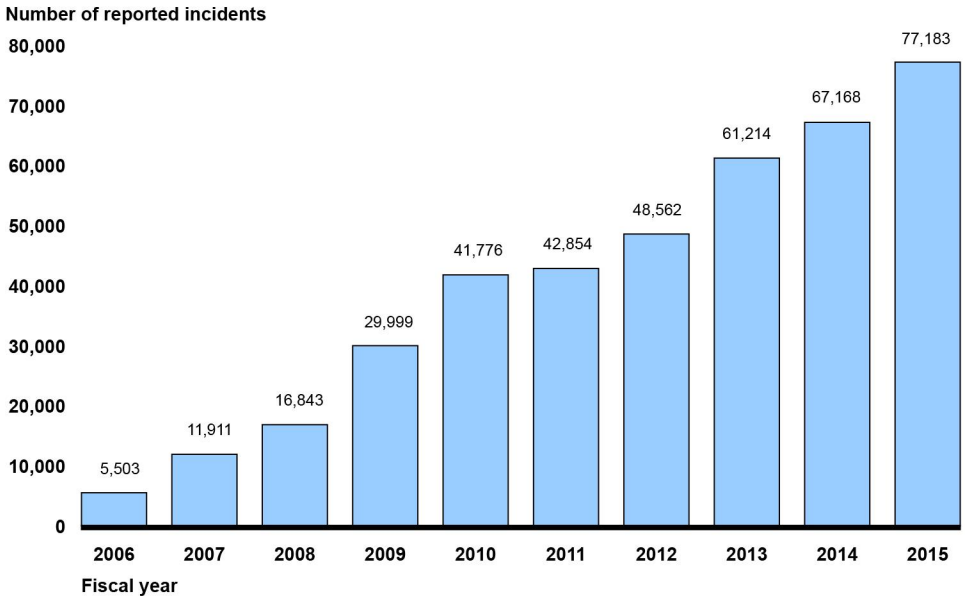
In addition, cyber threats and incidents to systems supporting the federal government are increasing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and

[2]The national vulnerability database is the U.S. government repository of standards-based vulnerability management data. These data enable automation of vulnerability management, security measurement, and compliance.

significant resources to pursue their objectives—pose increasing risks. Further underscoring this risk are increases in incidents that could threaten national security and public health and safety, or lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Such incidents may be unintentional, such as a service disruption due to equipment failure or natural event, or intentional, where for example, a hacker attacks a computer network or system.

The number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (U.S. CERT) has continued to increase—from 5,503 in fiscal year 2006 to 77,183 in fiscal year 2015, an increase of 1,303 percent (see fig. 1 below).

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Since 1997, we have designated federal information security as a government-wide high-risk area,[3] 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) collected, maintained, and shared by both federal and nonfederal entities.[4]

Over the last several years, we have made about 2,500 recommendations to agencies aimed at improving their implementation of information security controls. These recommendations identify actions for agencies to take in protecting their information and systems. For example, we have made recommendations for agencies to correct weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on their systems. We have also made recommendations for agencies to implement their information security programs and protect the privacy of PII held on their systems. However, many agencies continue to have weaknesses in implementing these controls, in part because many of these recommendations remain unimplemented. As of September 16, 2016, about 1,000 of our information security–related recommendations have not been implemented.

[3]GAO designates agencies and program areas as high-risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

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

Federal Law and Policy Establish a Framework for Protecting Federal Systems and Information

Several federal laws and policies—predominantly the Federal Information Security Modernization Act of 2014 and its predecessor, the Federal Information Security Management Act of 2002 (both referred to as FISMA)—provide a framework for protecting federal information and IT assets.

The purpose of both laws is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[5] The laws establish responsibilities for implementing the framework and assign those responsibilities to specific officials and agencies:

- The Director of the Office of Management and Budget (OMB) is responsible for developing and overseeing implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems. Since 2003, OMB has issued policies and guidance to agencies on many information security issues, including providing annual instructions to agencies and inspectors general for reporting on the effectiveness of agency security programs. More recently, OMB issued the *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* in October 2015,[6] which aims to strengthen federal civilian cybersecurity by (1) identifying and protecting high-value information and assets, (2) detecting and responding to cyber incidents in a timely manner, (3) recovering rapidly from incidents when they occur and accelerating the adoption of lessons learned, (4) recruiting and retaining a highly qualified cybersecurity workforce, and (5) efficiently acquiring and deploying existing and emerging technology. OMB also recently updated its Circular A-130 on

[5]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014); largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III of the E-Government Act of 2002 (Pub. L. No. 107-347, 116 Stat 2899, 2946 (Dec. 17, 2002)). As used here, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect

[6]OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

managing federal information resources to address protecting and managing federal information resources and on managing PII.[7]

- The head of each federal agency has overall responsibility for providing appropriate information security protections for the agency's information and information systems, including those collected, maintained, operated or used by others on the agency's behalf. In addition, the head of each agency is required to ensure that senior agency officials provide information security for the information and systems supporting the operations and assets under their control, and the agency chief information officer (CIO) is delegated the authority to ensure compliance with the law's requirements. The assignment of information security responsibilities to senior agency officials is noteworthy because it reinforces the concept that information security is a business function as well as an IT function.

Each agency is also required to develop, document, and implement an agency-wide information security program that involves an ongoing cycle of activity including (1) assessing risks, (2) developing and implementing risk-based policies and procedures for cost-effectively reducing information security risk to an acceptable level, (3) providing awareness training to personnel and specialized training to those with significant security responsibilities, (4) testing and evaluating effectiveness of security controls, (5) remedying known weaknesses, and (6) detecting, reporting, and responding to security incidents.

As discussed later, our work has shown that agencies have not fully or effectively implemented these programs and activities on a consistent basis.

- FISMA requires the National Institute of Standards and Technology (NIST) to develop information security standards and guidelines for agencies. To this end, NIST has developed and published federal information processing standards that require agencies to categorize their information and information systems according to the impact or magnitude of harm that could result if they are compromised[8] and

[7]OMB, Revision of OMB Circular A-130, *Managing Federal Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

[8]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

specify minimum security requirements for federal information and information systems.[9] NIST has also issued numerous special publications that provide detailed guidelines to agencies for securing their information and information systems.[10]

- In 2014, FISMA established the Department of Homeland Security's (DHS) oversight responsibilities, including (1) assisting OMB with oversight and monitoring of agencies' information security programs, (2) operating the federal information security incident center, and (3) providing agencies with operational and technical assistance.

Other cybersecurity-related laws were recently enacted, which include the following:

- 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 about cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities, including owners and operators of systems supporting critical infrastructure.[11]
- The Cybersecurity Enhancement Act of 2014, among other things, authorizes NIST to facilitate and support the development of voluntary standards to reduce cyber risks to critical infrastructure and, in coordination with OMB, to develop and encourage a strategy for the adoption of cloud computing services by the federal government.[12]
- The Cybersecurity Act of 2015, among other things, sets forth authority for enhancing the sharing of cybersecurity-related information among federal and non-federal entities, gives DHS's National Cybersecurity and Communications Integration Center responsibility for implementing these mechanisms, requires DHS to make intrusion and detection capabilities available to any federal

[9]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[10]For example, NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Rev. 1 (Gaithersburg, Md.: February 2010) and *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev. 4 (Gaithersburg, Md.: April 2013).

[11]Pub. L. No. 113-282, Dec. 18, 2014.

[12]Pub. L. No. 113-274, Dec. 18, 2014.

agency, and calls for agencies to assess their cyber-related workforce.[13]

Action Is Needed to Address Ongoing Cybersecurity Challenges

Our work has identified the need for improvements in the federal government's approach to cybersecurity. While the administration and agencies have acted to improve the protections over their information and information systems, additional actions are needed.

Federal agencies need to effectively implement risk-based entity-wide information security programs consistently over time. Since FISMA was enacted in 2002, agencies have been challenged to fully and effectively develop, document, and implement agency-wide programs to secure the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. For example, in fiscal year 2015, 19 of the 24 major federal agencies covered by the Chief Financial Officers Act of 1990[14] reported that information security control deficiencies were either a material weakness or significant deficiency[15] in internal controls over financial reporting. In addition, inspectors general at 22 of the 24 agencies cited information security as a major management challenge for their agency. The following actions will assist agencies in implementing their information security programs.

[13]The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

[14]The 24 major departments and 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 U.S. Agency for International Development. 31 U.S.C. § 901(b).

[15]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 deficiency, or combination of 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.

- *Enhance capabilities to effectively identify cyber threats to agency systems and information*. A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent.[16] The impairments included an inability to recruit and retain personnel with the appropriate skills, rapidly changing threats, continuous changes in technology, and a lack of government-wide information-sharing mechanisms. Addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.
- *Implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices.* We routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. Establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of federal agencies.
- *Patch vulnerable systems and replace unsupported software. Federal agencies consistently fail to apply critical security patches in a timely manner on their systems, sometimes years after the patch is available.* We also consistently identify instances where agencies use software that is no longer supported by their vendors. These shortcomings often place agency systems and information at significant risk of compromise since many successful cyberattacks exploit known vulnerabilities associated with software products. Using vendor-supported and patched software will help to reduce this risk.
- *Develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis.* The information security assessments performed for agency systems were sometimes based on interviews and document reviews, limited in

[16]GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

scope, and did not identify many of the security vulnerabilities that our examinations identified. Conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.

- *Strengthen oversight of contractors providing IT services.* As demonstrated by the Office of Personnel Management data breach of 2015, cyber attackers can sometimes gain entrée to agency systems and information through the agency's contractors or business partners. Accordingly, agencies need to ensure that their contractors and partners are adequately protecting the agency's information and systems. In August 2014, we reported that five of six selected agencies were inconsistent in overseeing the execution and review of security assessments that were intended to determine the effectiveness of contractor implementation of security controls, resulting in security lapses.[17] In 2016, agency chief information security officers (CISO) we surveyed reported that they were challenged to a large or moderate extent in overseeing their IT contractors and receiving security data from the contractors, thereby diminishing the CISOs' ability to assess how well agency information maintained by the contractors is protected.[18] Effectively overseeing and reviewing the security controls implemented by contractors and other parties is essential to ensuring that the organization's information is properly safeguarded.

The federal government needs to improve its cyber incident detection, response, and mitigation capabilities. Even agencies or organizations with strong security can fall victim to information security incidents due to previously unknown vulnerabilities that are exploited by attackers to intrude into an agency's information systems. Accordingly, agencies need to have effective mechanisms for detecting, responding to, and recovering from such incidents. The following actions will assist the federal government in building its capabilities for detecting, responding to, and recovering from security incidents.

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

[18]GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

- *DHS needs to expand capabilities, improve planning, and support wider adoption of its government-wide intrusion detection and prevention system.* In January 2016, we reported that DHS's National Cybersecurity Protection System (NCPS) had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.[19] In addition, adoption of these capabilities at federal agencies was limited. Expanding NCPS's capabilities for detecting and preventing malicious traffic, defining requirements for future capabilities, and developing network routing guidance would increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies.
- *Improve cyber incident response practices at federal agencies.* In April 2014 we reported that 24 major federal agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[20] For example, agencies did not determine the impact of incidents or take actions to prevent their recurrence. By developing complete policies, plans, and procedures for responding to incidents and effectively overseeing response activities, agencies will have increased assurance that they will effectively respond to cyber incidents.
- *Update federal guidance on reporting data breaches and develop consistent responses to breaches of personally identifiable information (PII).* As we reported in December 2013, eight selected agencies did not consistently implement policies and procedures for responding to breaches of PII.[21] For example, none of the agencies documented the evaluation of incidents and lessons learned. In addition, OMB's guidance to agencies to report each PII-related incident—even those with inherently low risk to the individuals affected—within 1 hour of discovery may cause agencies to expend resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches. Updating

[19]GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

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

[21]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).

guidance and consistently implementing breach response practices will improve the effectiveness of government-wide and agency-level data breach response programs.

The federal government needs to expand its cyber workforce planning and training efforts. Ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge. These actions can help meet this challenge:

- *Enhance efforts for recruiting and retaining a qualified cybersecurity workforce.* This has been a long-standing dilemma for the federal government. In 2012, agency chief information officers and experts we surveyed cited weaknesses in education, awareness, and workforce planning as a root cause in hindering improvements in the nation's cybersecurity posture.[22] Several experts also noted that the cybersecurity workforce was inadequate, both in numbers and training. They cited challenges such as the lack of role-based qualification standards and difficulties in retaining cyber professionals. In 2016, agency CISOs we surveyed reported that difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; and ensuring security personnel have appropriate skills and expertise pose challenges to their abilities to carry out their responsibilities effectively.[23]
- *Improve cybersecurity workforce planning activities at federal agencies.* In November 2011, we reported that only five of eight selected agencies had developed workforce plans that addressed cybersecurity.[24] Further, agencies reported challenges with filling cybersecurity positions, and only three of the eight had a department-wide training program for their cybersecurity workforce.

[22]GAO, Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[23]GAO-16-686.

[24]GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

In summary, federal law and policy set forth a framework for addressing cybersecurity risks to federal systems. However, implementation of this framework has been inconsistent, and additional action is needed to address ongoing challenges. Specifically, agencies need to address control deficiencies and fully implement organization-wide information security programs, cyber incident response and mitigation efforts need to be improved across the government, and establishing and maintaining a qualified cybersecurity workforce needs to be a priority.

Chairman Donilon, Vice Chair Palmisano, and distinguished members of the Commission, this concludes my prepared statement. I would be happy to answer any questions you have.

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), Chris Businsky, Franklin Jackson, Kenneth A. Johnson, Lee McCracken, Scott Pettis, and Adam Vodraska.

Appendix I: Accessible Data

Data Tables

Data Table for Highlights Figure and Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015

Fiscal year	Number of reported incidents
2006	5503
2007	11911
2008	16843
2009	29999
2010	41776
2011	42854
2012	48562
2013	61214
2014	67168
2015	77183