United States Government Accountability Office

Testimony

Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, June 24, 2015

CYBERSECURITY

Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies

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

Accessible Version

June 24, 2015

CYBERSECURITY

Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies

GAO Highlights

Highlights of GAO-15-725T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, 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. Federal information and systems face an evolving array of cyber-based threats, and recent data breaches at federal agencies highlight the impact that can result from ineffective security controls.

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. 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) challenges facing federal agencies in securing their systems and information and (2) government-wide initiatives, including those led by DHS, 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-15-725T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified a number of challenges federal agencies face in addressing threats to their cybersecurity, including the following:

- Designing and implementing a risk-based cybersecurity program.
- Enhancing oversight of contractors providing IT services.
- Improving security incident response activities.
- Responding to breaches of personal information.
- 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, including sensitive personal information, will be at an increased risk of compromise from cyber-based attacks and other threats.

In an effort to bolster cybersecurity across the federal government, several government-wide initiatives, spearheaded by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are under way. These include the following:

- **Personal Identity Verification:** In 2004, the President directed the establishment of a government-wide standard for secure and reliable forms of ID for federal employees and contractor personnel who access government facilities and systems. Subsequently, OMB directed agencies to issue personal identity verification credentials 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 for accessing agency systems.
- **Continuous Diagnostics and Mitigation:** DHS, in collaboration with the General Services Administration, has established a government-wide contract for agencies to purchase tools that are intended to identify cybersecurity risks on an ongoing basis. These tools can support agencies' efforts to monitor their networks for security vulnerabilities and generate prioritized alerts to enable agency staff to mitigate the most critical weaknesses. The Department of State adopted a continuous monitoring program, and in 2011 GAO reported on the benefits of the program and challenges the department faced in implementing its approach.
- **National Cybersecurity Protection System (NCPS):** This system, also referred to as EINSTEIN, is to include capabilities for monitoring network traffic and detecting and preventing intrusions, among other things. GAO has ongoing work reviewing the implementation of NCPS, and preliminary observations indicate that implementation of the intrusion detection and prevention capabilities may be limited and DHS appears to have not fully defined requirements for future capabilities.

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, "defense in depth" approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

Thank you for inviting me to testify at today's hearing on the Department of Homeland Security's (DHS) efforts to secure federal information systems. 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 the Office of Personnel Management (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 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) cybersecurity challenges that federal agencies face in securing their systems and information and (2) government-wide initiatives, including those led by DHS, 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 DHS's EINSTEIN 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 evidence to provide a reasonable basis for our findings and conclusions

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

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

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

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 business 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 requires federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Cyber Threats to Federal Systems

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.

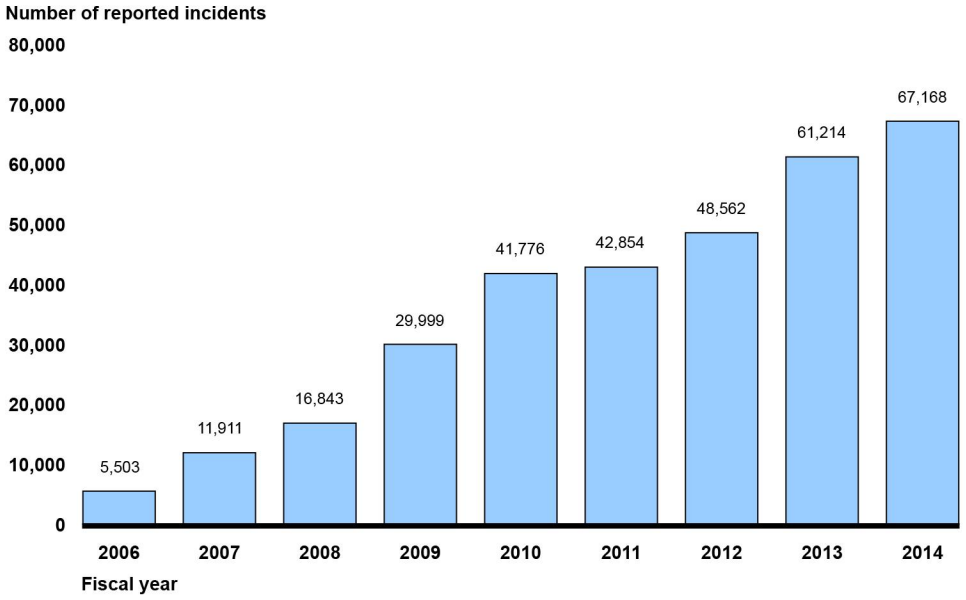
These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques— or exploits—that may adversely affect federal information, computers, software, networks, and operations.

Since fiscal year 2006, the number of information security incidents affecting systems supporting the federal government has steadily

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

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-15-725T

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.

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[4] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over

[4]These 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.

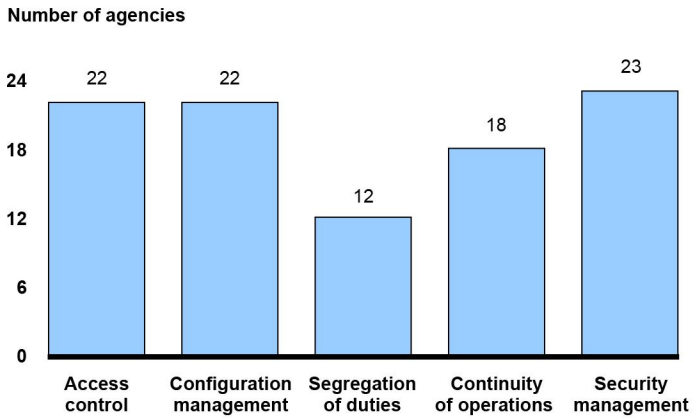
their financial reporting.[5] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency.

As we testified in April 2015, for fiscal year 2014, most of the agencies had weaknesses in the five key security control categories.[6] 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. 2.)

[5]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.

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

Figure 2: 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-15-725T

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. GAO 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.[7] 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 OMB, in conjunction with DHS,

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

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 agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[8] 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.[9] 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. We also made two recommendations to DHS concerning government-wide incident response practices. DHS concurred with the recommendations and, to date, has implemented one of them.
- **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.[10] 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

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

[9]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.

[10]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).

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 implemented or not fully implemented their information security programs.[11] 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 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, the National Institute of Standards and Technology (NIST) defined requirements for such personal identity verification (PIV) credentials based on "smart cards"—plastic cards with integrated circuit chips to

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

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 access to federal facilities and information systems.[12] 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, who 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.[13]

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

[12]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).

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

iPost.[14] We determined that State's implementation of iPost had improved 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 1.[15]

Table 1: 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-15-725T

[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.

[14]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)

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

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 was meeting its objectives.[16] 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 mandated by Congress. 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.[17] 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.

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

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

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 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.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you may 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), Bradley Becker, Christopher Businsky, Nancy Glover, Rosanna Guerrero, Kush Malhotra, and Lee McCracken.

Appendix I: Accessible Data

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

Fiscal year	Number of reported incidents
2006	5,503
2007	11,911
2008	16,843
2009	29,999
2010	41,776
2011	42,854
2012	48,562
2013	61,214
2014	67,168

Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-725T

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

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

Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-725T