United States Government Accountability Office

Testimony

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

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

# INFORMATION SECURITY

# Department of Education and Other Federal Agencies Need to Better Implement Controls

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

November 17, 2015

# INFORMATION SECURITY

## Department of Education and Other Federal Agencies Need to Better Implement Controls

GAO Highlights

Highlights of GAO-16-228T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

## Why GAO Did This Study

The federal government faces an evolving array of cyber-based threats to its systems and data, and data breaches at federal agencies have compromised sensitive personal information, affecting millions of people. Education, in carrying out its mission of serving America's students, relies extensively on IT systems that collect and process a large amount of sensitive information. Accordingly, it is important for federal agencies such as Education to implement information security programs that can help protect systems and networks. GAO has identified federal information security as a government-wide high-risk area since 1997, and in February 2015 expanded this to include protecting the privacy of personally identifiable information.

This statement provides information on cyber threats facing federal systems and information security weaknesses identified at federal agencies, including Education. In preparing this statement, GAO relied on previously published work and updated data on security incidents and federal cybersecurity efforts.

## What GAO Recommends

Over the past 6 years, GAO has made about 2,000 recommendations to federal agencies to correct weaknesses and fully implement agency-wide information security programs. Agencies have implemented about 58 percent of these recommendations. Agency inspectors general have also made a multitude of recommendations to assist their agencies.

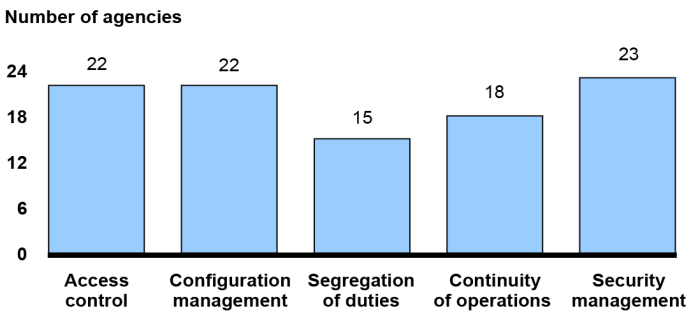
View GAO-16-228T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

## What GAO Found

Cyber-based risks to federal systems and information can come from unintentional threats, such as natural disasters, software coding errors, and poorly trained or careless employees, or intentional threats, such as disgruntled insiders, hackers, or hostile nations. These threat sources may exploit vulnerabilities in agencies' systems and networks to steal or disclose sensitive information, among other things. Since fiscal year 2006, the number of reported information security incidents affecting federal systems has steadily increased, rising from about 5,500 in fiscal year 2006 to almost 67,200 in fiscal year 2014. At the Department of Education, the number of incidents reported since 2009 has fluctuated, but generally increased.

GAO reported in September 2015, that most of 24 major agencies (including Education) had weaknesses in at least three of five major categories of information security controls for fiscal year 2014. These are controls intended to (1) limit unauthorized access to agency systems and information; (2) ensure that software and hardware are authorized, updated, monitored, and securely configured; (3) appropriately divide duties so that no single person can control all aspects of a computer-related operation; (4) establish plans for continuing information system operations in the event of a disaster, and (5) provide a security management framework for understanding risks and ensuring that controls are selected, implemented, and operating as intended. The figure below shows the number of agencies with weaknesses in these control categories.

**Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014**




Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-228T

In addition, 19 agencies—including Education—reported that information security control deficiencies were either a material weakness or a significant deficiency for fiscal year 2014. Further, inspectors general for 23 of 24 agencies, including Education, cited information security as a major management challenge. In prior reports, GAO and inspectors general have made thousands of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain open. Until agencies implement these recommendations, sensitive information will remain at risk of unauthorized disclosure, modification, or destruction.

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

Thank you for the opportunity to testify at today's hearing on information security at the Department of Education (Education). As requested, my statement today will address cyber threats facing federal systems and information and security control weaknesses that have been identified at federal agencies, including Education.

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

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

In preparing this statement, we relied on our previous work addressing cyber threats and federal information security efforts. We also relied on the number of incidents previously reported by Education; information technology spending previously reported by the Office of Management and Budget (OMB) and federal agencies; and recently reported data from

[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).

the Cybersecurity Sprint.[3] The prior reports cited throughout this statement contain detailed discussions of the scope of the work and the methodology used to carry it out.

All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A list of related GAO products is provided in attachment I.

## Background

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

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

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

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

- 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 2014),[4] which, among other things, 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. This includes protections for information collected or maintained on behalf of the agency and information systems used or operated by a contractor of an agency or other organization on behalf of an agency.

In addition, the act continues the requirement for federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other organization on behalf of an agency.

The act also authorizes the Department of Homeland Security (DHS) to (1) assist the Office of Management and Budget (OMB) with overseeing and monitoring agencies' implementation of security requirements; (2) operate the federal information security incident center; and (3) provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities.

## Department of Education Relies on Information Technology Systems Containing Sensitive Information

The mission of the Department of Education is to serve America's students and promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. In carrying out its mission, the department is responsible for four major types of activities:

- establishing policies relating to federal financial aid for education, administering distribution of those funds, and monitoring their use;

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

- collecting data and overseeing research on America's schools and disseminating this information to Congress, educators, and the general public;
- identifying the major issues and problems in education and focusing national attention on them; and
- enforcing federal statutes that prohibit discrimination in programs and activities receiving federal funds and ensuring equal access to education for every individual.

To support these activities, the department relies on a variety of information technology (IT) systems and infrastructure. Moreover, the department's systems contain large volumes of sensitive information such as personnel records, financial information, and personally identifiable information. According to a fiscal year 2015 inspector general report, about 70 million users, which included students and borrowers, utilized the systems supporting the department's federal student aid program.[5]

## Cyber Threats to Federal Systems Continue to Evolve amid Increasing Numbers of Incidents

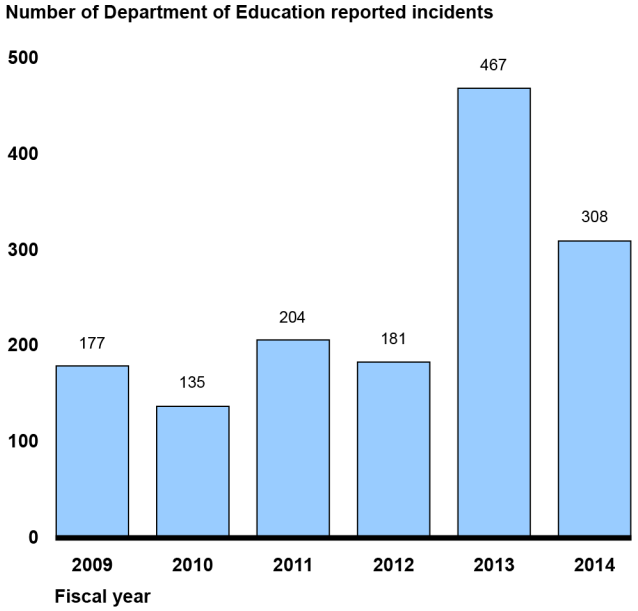
Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats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

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary or personal gain or pursuing a political, economic, or military advantage. For example, insiders can pose threats because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system, steal system data, or disclose sensitive information without authorization. The insider threat includes inappropriate actions by contractors hired by the organization, as well as careless or poorly trained employees.

[5]Department of Education, Office of Inspector General, *The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014,* Report No. ED-OIG/A11O0001 (Washington, D.C.: November 2014).

As we reported in February 2015,[6] since fiscal year 2006, the number of information security incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT)[7] affecting systems supporting the federal government has steadily increased each year. Specifically, the number of reported incidents rose from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent. At Education, the number of reported incidents has fluctuated during the period from fiscal year 2009 to fiscal year 2014, with the department reporting 308 incidents in fiscal year 2014 after reaching a high of 467 in fiscal year 2013.

**Figure 1: Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team by the Department of Education, Fiscal Years 2009 through 2014**



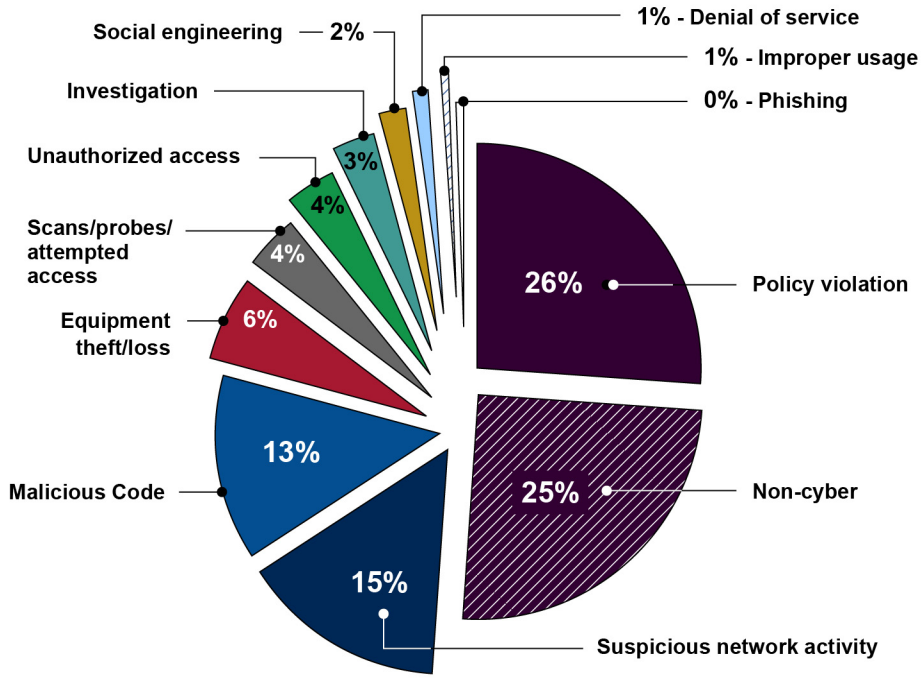

Source: GAO analysis of United States Computer Emergency Readiness Team data for Education for fiscal years 2009 to 2014. | GAO-16-228T

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

[6]GAO-15-290.

[7]When incidents occur, agencies are to notify US-CERT.

**Figure 2: Fiscal Year 2014 Information Security Incidents by Type as Reported by the Department of Education**




Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-16-228T

The types of incidents reported by Education are generally consistent with those reported by the other 23 major federal agencies, with a few exceptions. For example, at 26 percent, policy violations constituted the highest percentage of incidents reported by Education for fiscal year 2014. Policy violations involve incidents of mishandling data in storage or transit, such as digital PII records. In contrast, only 17 percent of incidents reported by the 24 major federal agencies were policy violations. The second highest percentage of incidents reported by Education was non-cyber incidents, at 25 percent, which was the same percentage reported by federal agencies. Non-cyber incidents are those that include PII spillages or possible mishandling of PII which involve hard copies or printed material as opposed to digital records.

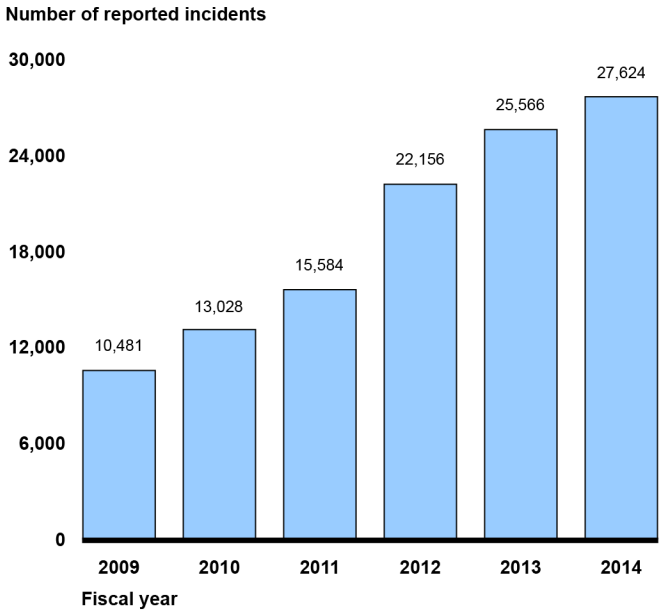
Suspicious network activity, at 15 percent, and malicious code, at 13 percent, were the third and fourth highest percentages of incidents that Education reported for fiscal year 2014. Suspicious network activity refers to incidents identified through Einstein[8] data analyzed by US-CERT, and malicious code incidents are successful executions or installations of malicious software which are not immediately quarantined and cleaned by preventative measures such as antivirus tools. Suspicious network activity made up 3 percent of the 24 major federal agencies' reported incidents, and malicious code constituted 11 percent of the incidents federal agencies reported for fiscal year 2014.

Finally, only 4 percent of the incidents reported by Education were for scans/probes/attempted access, which was the most widely reported type of incident by federal agencies (excluding non-cyber incidents). This type of incident can involve identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit.

Furthermore, the number of reported security incidents involving PII at federal agencies has more than doubled in recent years—from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014. (See fig 3.)

[8]Einstein is a system of systems that is intended to deliver a range of capabilities including intrusion detection and prevention, analytics, and information sharing. The goal of Einstein is to provide the federal government with an early warning system, improved situational awareness of intrusion threats, near real-time identification, and prevention of malicious cyber activity.

**Figure 3: Incidents Involving Personally Identifiable Information Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies for Fiscal Years 2009 through 2014**




Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2009-2014. | GAO-16-228T

These incidents and others like them can adversely affect national security and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Examples at other agencies highlight the impact of such incidents:

- In June 2015, the Office of Personnel Management (OPM) reported that an intrusion into its systems affected the personnel records of about 4.2 million current and former federal employees. The Director stated that a separate but related incident involved the agency's background investigation systems and compromised background investigation files for 21.5 million individuals.

- In June 2015, the Commissioner of the Internal Revenue Service testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to officials, criminals used taxpayer-specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. This data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the

agency reported this number to be about 114,000 and that an additional 220,000 accounts had been inappropriately accessed, which brings the total to about 330,000 accounts.

- In April 2015, the Department of Veterans Affairs' Office of Inspector General reported that two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.[9]

- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.[10]

- 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.[11]

- In October 2013, a wide-scale cybersecurity breach involving a U.S. Food and Drug Administration system occurred that exposed the PII of 14,000 user accounts.[12]

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

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

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

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

## Similar to Other Agencies, Information Security Weaknesses Place Education's Systems and Sensitive Data at Risk

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that federal agencies, such as Education, take appropriate steps to secure their systems and information. We and agency inspectors general have identified numerous weaknesses in protecting federal information systems and information. Agencies, including Education, continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results.

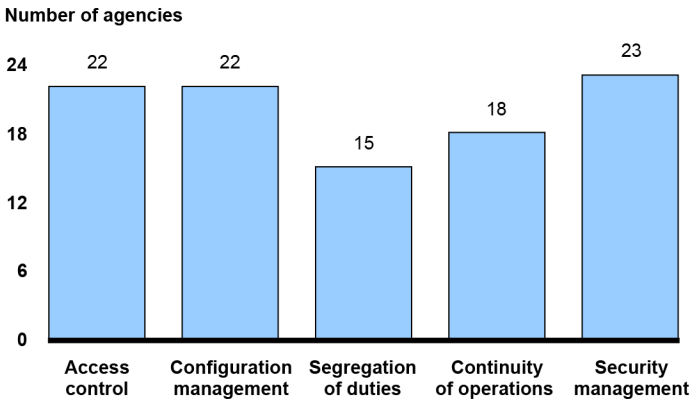
As we reported in September 2015, for fiscal year 2014 most of the 24 agencies covered by the Chief Financial Officers Act,[13] including Education, had weaknesses in most of the five major categories of information system controls.[14] These control categories are: (1) access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (2) configuration management controls, intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and assure that software is current and known vulnerabilities are patched; (3) segregation of duties, which prevents a single individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; (4) contingency planning,[15] which helps avoid significant disruptions in computer-dependent operations; and (5) agency-wide security management, which provides a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended. (See fig. 4.)

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

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

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

**Figure 4: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014**




Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-228T

- **Access controls:** For fiscal year 2014, Education and 21 other agencies had weaknesses in electronic and physical controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby increasing their risk of unauthorized use, modification, disclosure, and loss. Specifically, Education's inspector general reported weaknesses in several key access control elements, including protecting the boundaries of its information systems and handling incidents. For example, the department did not implement controls to verify the security of non-government furnished equipment connecting to its network via virtual private client programs prior to authentication.

- **Configuration management:** For fiscal year 2014, 22 agencies, including Education, had weaknesses reported in controls that are intended to ensure that only authorized and fully tested software is placed in operation, software and hardware is updated, information systems are monitored, patches are applied to these systems to protect against known vulnerabilities, and emergency changes are documented and approved. For example, the department's configuration management guidance had not been updated since 2005 and its IT security baseline configuration guidance had not been updated since 2009.

- **Segregation of duties:** Fifteen agencies had weaknesses reported in controls for segregation of duties, although Education was not one of

them. These controls are the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a computer-related operation and thereby take unauthorized actions or gain unauthorized access to assets or records.

- **Continuity of operations:** Education and 17 other agencies had weaknesses reported in controls for their continuity of operations practices for fiscal year 2014. For example, Education did not consistently document the IT recovery procedures for its systems in accordance with National Institute of Standards and Technology (NIST) guidelines and departmental policies. In addition, the department did not consistently perform and document testing of contingency plans for certain systems.

- **Security management:** For fiscal year 2014, 23 agencies, including Education, had weaknesses reported in security management, which is an underlying cause for information security control deficiencies identified at federal agencies. An agency-wide security program, as required by FISMA, provides a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. FISMA also requires agencies to develop and document an inventory of major systems. Regarding Education, the inspector general reported weaknesses in several key elements, including developing, documenting, and updating an inventory of its systems; periodically assessing risks to its systems; ensuring staff receive security awareness training; and remediating information security weaknesses. For example, the department did not implement corrective actions in a timely manner including 15 corrective actions that were completed late without a revised planned completion date.

In addition, independent reviews at the 24 agencies continued to highlight deficiencies in their implementation of information security policies and procedures. Specifically, for fiscal year 2014, 19 agencies—including Education—reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls

over their financial reporting.[16] Education was 1 of 12 agencies that reported that such weaknesses constituted a significant deficiency—which is less severe than a material weakness but important enough to merit attention by those charged with governance. Further, 23 of 24 inspectors general for the agencies, including Education, cited information security as a "major management challenge" for their agency.

In accordance with their responsibilities under FISMA, inspectors general at the 24 agencies continued to report on their respective agencies' fiscal year 2014 implementation of information security programs for these 11 program components:[17]

- **Risk management:** Inspectors general reported that program components for addressing risks at 17 agencies, including Education, were established. However, Education's inspector general identified exceptions. For example, the department's risk management program was not fully implemented and the process for system authorization needed improvement.
- **Configuration management:** Sixteen agencies, including Education, had established elements of their programs for managing changes to hardware and software. Education's inspector general noted exceptions in the department's configuration management policies, procedures, and plans and reported that they did not always comply with NIST and departmental guidance.
- **Incident response and reporting:** Twenty-one agencies, including Education, had established a program for detecting, reporting, and responding to security incidents. The Education inspector general noted that improvements were needed in the department's reporting

[16]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, but 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.

[17]According to OMB, one inspector general did not report on its agency's contingency planning, contractor systems, and security capital planning programs for fiscal year 2014. Therefore, the results of only 23 agencies were included for these areas.

of incidents to the US-CERT and law enforcement agencies. For example, the inspector general reported that 4 of 45 sampled incidents were not reported to the US-CERT, as required.

- **Security training:** Along with 19 other agencies, Education had established a program for providing security training to staff.
- **Remedial actions:** Education and 18 other agencies had established program components for addressing deficiencies in information security policies, procedures, and practices.
- **Remote access:** Twenty-one agencies, including Education, had established program components for managing remote access to their networks. However, Education's inspector general also reported exceptions with this component. For example, the department lacked restrictions for virtual private network client programs on non-government-furnished equipment. In addition, it had not fully implemented two-factor authentication, and improvements were needed in the use of mobile devices when accessing the department's network.
- **Identity and access management:** Education, along with 15 other agencies, established program components for ensuring that users were properly identified and authenticated when accessing agency resources. However, Education's inspector general reported that the department needed to improve its password authentication process and had not fully implemented logical access controls.
- **Continuous monitoring:** Nineteen agencies, including Education, had established program components for continuously monitoring the effectiveness of security policies, procedures, and practices.
- **Contingency planning:** Education and 16 other agencies had established program components for ensuring continuity of operations for information systems in the event of a disaster or other unforeseen disruptions. However, Education's inspector general reported that the department's contingency plans were not always complete, and the process for testing the plans needed improvements.
- **Contractor systems:** At 17 agencies, including Education, inspectors general reported that program components for monitoring contractor systems had been established.

- **Security capital planning:** Education, along with 18 other agencies, had established program components for capital planning and investment for information security.

As we noted in our September 2015 report on federal information security, the annual FISMA reporting guidance that OMB and DHS provided to inspectors general was not complete, resulting in different interpretations among the inspectors general and inconsistent reporting results.[18] As a result, responses from inspectors general may not always be comparable or provide a clear government-wide picture of agencies' security implementation.

Accordingly, we recommended that OMB, in consultation with DHS and other stakeholders, enhance the reporting guidance so that ratings would be consistent and comparable across agencies. OMB generally concurred with our recommendation and stated that it would continue to work with DHS and other stakeholders to refine the FISMA reporting metrics and enhance reporting guidance.

Over the last several years, we and agency inspectors general have made thousands of recommendations to agencies aimed at improving their implementation of information security controls. For example, we have made about 2,000 recommendations over the last 6 years. Agency inspectors general have also made a multitude of recommendations to assist their agencies. Many agencies continue to have weaknesses in implementing these controls in part because many of these recommendations remain unimplemented. For example, agencies have not yet implemented about 42 percent of the recommendations we have made during the last 6 years. Until federal agencies take actions to implement the recommendations made by us and the inspectors general—federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

## Federal Efforts Are Intended to Improve Cybersecurity

Although weaknesses continue to exist, the federal government has initiated or continued several efforts to protect federal information and information systems. The White House, OMB, and federal agencies have

[18]GAO-15-714.

launched several government-wide initiatives that are intended to enhance information security at federal agencies. These key efforts include the following.

Cybersecurity Cross-Agency Priority (CAP) Goals. Initiated in 2012, CAP goals are an effort to focus agencies' cybersecurity activity on the most effective controls. Education reported the following levels of performance with respect to metrics related to the CAP goals:

- **Trusted Internet Connections (TIC):** Aims to improve the federal government's security posture through the consolidation of external telecommunication connections by establishing a set of baseline security capabilities through enhanced monitoring and situational awareness of all external network connections. OMB established a 100 percent target for implementing TIC capabilities for fiscal year 2014 and reported that the 24 agencies covered by the Chief Financial Officers Act achieved an overall implementation rate of 92 percent. For fiscal year 2014, Education reported a 95 percent implementation rate.

- **Continuous Monitoring of Federal Information Systems:** Intended to provide near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk management decisions based on increased situational awareness. OMB established a fiscal year 2014 target of 95 percent and reported that overall the 24 agencies had achieved 92 percent implementation. Education reported 98 percent continuous monitoring of its assets at the end of fiscal year 2014.

- **Strong Authentication:** Intended to increase the use of federal smartcard credentials, such as personal identity verification and common access cards that provide multifactor authentication and digital signature and encryption capabilities. Strong authentication can provide a higher level of assurance when authorizing users' access to federal information systems. For fiscal year 2014, OMB established a 75 percent implementation rate, but indicated that the 24 agencies had implemented strong authentication for a combined 72 percent of their users. Education reported an 85 percent implementation rate at the end of fiscal year 2014.

**The 30-Day Cybersecurity Sprint.** In June 2015, in response to the OPM security breaches and to improve federal cybersecurity and protect systems against evolving threats, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint and instructed agencies to

immediately take a number of steps to further protect federal information and to improve the resilience of federal networks. One step was to accelerate the implementation of multi-factor authentication, such as the use of personal identity verification cards to gain access to federal networks, systems, and data. According to a report by the Executive Office of the President, the percentage of Education's users who used strong authentication decreased to 57 percent, one of only four agencies to show a decrease following the sprint.[19]

**Agency Spending on Cybersecurity Activities.** According to OMB, the 24 agencies covered by the Chief Financial Officers Act reported spending about $12.7 billion on cybersecurity activities in fiscal year 2014.[20] Of this amount, the 23 civilian agencies[21] reportedly spent about $3.75 billion or about 9 percent of the amount the agencies reportedly spent on information technology in fiscal year 2014.[22] For fiscal year 2014, Education reportedly spent about $32 million on cybersecurity, or roughly 5 percent of the amount it reportedly spent on information technology.[23] The agencies reported spending amounts for three major categories of cybersecurity activities: preventing malicious cyber activity; detecting, analyzing, and mitigating intrusions; and shaping the

[19]Executive Office of the President of the United States, *Cybersecurity Sprint Results* (Washington, D.C.: July 2015).

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

[21]We excluded the Department of Defense from this analysis because the amount it reportedly spent on cybersecurity activities dwarfed the combined amount spent by the other 23 agencies and its inclusion would inappropriately skew the results.

[22]The 9 percent amount was computed by dividing $3.75 billion the 23 civilian agencies spent on cybersecurity activities by the amount they reportedly spent on information technology in fiscal year 2014, which according to the IT Dashboard was about $43.9 billion.

[23]The 5 percent amount was computed by dividing the $32 million spent on cybersecurity activities according to OMB by the amount spent on information technology (about $630 million according to the IT Dashboard).

cybersecurity environment.[24] Of the about $32 million it reportedly spent on cybersecurity activities, Education spent 34 percent on preventing malicious activity; 63 percent on detecting, analyzing, and mitigating intrusions; and 3 percent on shaping the cybersecurity environment.

In conclusion, the dangers posed by a wide array of cyber threats facing the nation are heightened by weaknesses in the federal government's approach to protecting its systems and information. While federal agencies, including the Department of Education, have established information security programs, weaknesses in these programs persist, and more needs to be done to fully implement them and to address existing weaknesses. In particular, implementing outstanding inspector general and GAO recommendations will strengthen agencies' ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

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

## Contact and Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff members who contributed to this statement include Larry Crosland, Assistant Director; Christopher Businsky; Rosanna Guerrero; Fatima Jahan; and Lee McCracken.

[24]**Preventing malicious cyber activity** is an area of spending that pertains to monitoring federal government systems and networks and protecting the data within from both external and internal threats. **Detecting, analyzing, and mitigating intrusions** is an area of spending on systems and processes used to detect security incidents, analyze the threat, and attempt to mitigate possible vulnerabilities. **Shaping the cybersecurity environment** is an area of spending on improving the efficacy of current and future information security efforts, such as building a strong information security workforce and supporting broader IT security efforts.

# Attachment I: Related GAO Products

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 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.