



September 2015

FEDERAL INFORMATION SECURITY

Agencies Need to Correct Weaknesses and Fully Implement Security Programs

Accessible Version

GAO Highlights

Highlights of [GAO-15-714](#), a report to congressional committees

Why GAO Did This Study

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. In February 2015, in its high risk update, GAO further expanded this area to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

FISMA required federal agencies to develop, document, and implement an agency-wide information security program. The act also assigned OMB with overseeing agencies' implementation of security requirements.

FISMA also included a provision for GAO to periodically report to Congress on (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) agencies' implementation of FISMA requirements. GAO analyzed information security-related reports and data from 24 federal agencies, their inspectors general, and OMB; reviewed prior GAO work; examined documents from OMB and DHS; and spoke to agency officials.

What GAO Recommends

GAO is recommending that OMB, in consultation with DHS and others, enhance security program reporting guidance to inspectors general so that the ratings of agency security performance will be consistent and comparable. OMB generally concurred with our recommendation.

View [GAO-15-714](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

September 2015

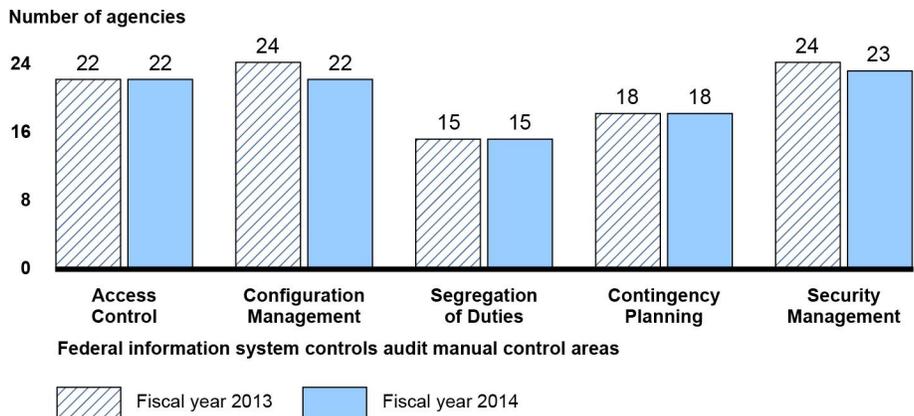
FEDERAL INFORMATION SECURITY

Agencies Need to Correct Weaknesses and Fully Implement Security Programs

What GAO Found

Persistent weaknesses at 24 federal agencies illustrate the challenges they face in effectively applying information security policies and practices. Most agencies continue to have weaknesses in (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.). These deficiencies place critical information and information systems used to support the operations, assets, and personnel of federal agencies at risk, and can impair agencies' efforts to fully implement effective information security programs. In prior reports, GAO and inspectors general have made hundreds of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented.

Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

Federal agencies' implementation in fiscal years 2013 and 2014 of requirements set by the *Federal Information Security Management Act of 2002* (FISMA) was mixed. For example, most agencies had developed and documented policies and procedures for managing risk, providing security training, and taking remedial actions, among other things. However, each agency's inspector general reported weaknesses in the processes used to implement FISMA requirements. In addition, to comply with FISMA's annual reporting requirements, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) provide guidance to the inspectors general on conducting and reporting agency evaluations. Nevertheless, GAO found that this guidance was not always complete, leading to inconsistent application by the inspectors general. For example, because it did not include criteria for making overall assessments, inspectors general inconsistently reported agency security performance.

Contents

Letter	1
Background	4
Continued Weaknesses Place Federal Agencies' Information and Information Systems at Risk	11
Agencies' Implementation of FISMA 2002 Requirements Was Mixed	31
Conclusions	54
Recommendation for Executive Action	55
Agency Comments and Our Evaluation	55

Appendix I: Objectives, Scope, and Methodology	57
Appendix II: Cyber Threats and Exploits	59
Appendix III: Number of Agency and Contractor-Operated Systems by Impact Level	62
Appendix IV: Comments from the Social Security Administration	63
Appendix V: GAO Contact and Staff Acknowledgments	64
Appendix VI: Accessible Data	65
Data Tables	65
Agency Comments	67

Tables	
Table 1: Critical Elements for Access Control to Computer Resources	19
Table 2: National Cybersecurity Protection System Capabilities	26
Table 3: Number of Agencies Documenting Information Security Policies and Procedures for Fiscal Years 2013 and 2014	34
Table 4: Agency Incident Reporting and Response Practices as Reported for Fiscal Years 2013 and 2014	42
Table 5: Total Number of Agency and Contractor-Operated Systems Reported for Fiscal Years 2013 and 2014 by Impact Level	45
Table 6: Reported Fiscal Year 2014 Federal Agencies Cybersecurity Spending by Major Category (amounts in millions)	48
Table 7: NIST FISMA-Related Publications	49
Table 8: Sources of Cybersecurity Threats	59
Table 9: Types of Cyber Exploits	60

Table 10: Cyber Events Characterized by Tactics, Techniques, and Practices	61
Table 11: Number of Agency and Contractor-Operated Systems in Fiscal Year 2014, by Impact Level	62
Data Table for Highlights Figure: Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014	65
Data Table for Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014	65
Data Table for Figure 2: Information Security Incidents by Category, Fiscal Year 2014	65
Data Table for Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014	66
Data Table for Figure 4: Examples of Agencies' Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014	66
Data Table for Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014	66
Data Table for Figure 6: Agencies' Reported Cybersecurity Spending	67

Figures

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014	12
Figure 2: Information Security Incidents by Category, Fiscal Year 2014	13
Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014	18
Figure 4: Examples of Agencies' Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014	32
Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014	40
Figure 6: Agencies' Reported Cybersecurity Spending	47
Accessible Text for Appendix: IV: Comments from the Social Security Administration	67

Abbreviations

CAP	cross-agency priority
CDM	Continuous Diagnostics and Mitigation
CFO Act	<i>Chief Financial Officers Act of 1990</i>
CIO	chief information officer
DHS	Department of Homeland Security

DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
Education	Department of Education
E-Gov Cyber	E-Gov Cyber and National Security Unit
EPA	Environmental Protection Agency
FedRAMP	Federal Risk and Authorization Management Program
FISCAM	<i>Federal Information System Controls Audit Manual</i>
FISMA 2002	<i>Federal Information Security Management Act of 2002</i>
FISMA 2014	<i>Federal Information Security Modernization Act of 2014</i>
GSA	General Services Administration
HHS	Department of Health and Human Services
HSPD-12	Homeland Security Presidential Directive 12
HUD	Department of Housing and Urban Development
NASA	National Aeronautics and Space Administration
NCPS	National Cybersecurity Protection System (EINSTEIN)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
POA&M	plan of action and milestones
SBA	Small Business Administration
SSA	Social Security Administration
State	Department of State
TIC	Trusted Internet Connections
Treasury	Department of the Treasury
USAID	U.S. Agency for International Development.
US-CERT	United States Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 29, 2015

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The widespread use of the Internet has changed the way that our government, our nation, and the rest of the world communicate and conduct business. While the benefits have been enormous, this connectivity—without effective cybersecurity—can also pose significant risks to computer systems and networks as well as to the critical operations and key infrastructures they support. Resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructures¹ could be disrupted, with potentially catastrophic effects.

The emergence of increasingly sophisticated cyber threats underscores the need to manage and bolster the security of federal information systems. For example, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using multiple means such as cyber, physical, or deception to achieve its objectives—pose increasing risks. In addition, the number and

¹Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. These critical infrastructures are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

types of cyber threats are on the rise. The recent attack on federal personnel and background investigation files that breached the personally identifiable information (PII)² for more than 20 million federal employees and contractors illustrates the need for strong security over information and systems. Further, in February 2015, the Director of National Intelligence testified³ that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.

Since 1997, we have designated federal information security as a government-wide high-risk area,⁴ and in 2003,⁵ expanded this area to include computerized systems supporting the nation's critical infrastructure. In our 2015 High-Risk update,⁶ we further expanded this area to include protecting the privacy of PII.

The *Federal Information Security Management Act of 2002* (FISMA 2002) established information security program and evaluation requirements for federal agencies in the executive branch.⁷ FISMA 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). Each year, each federal agency is to have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. The results of the evaluation, performed by the agency's inspector general or independent external auditor, are to be reported annually to

²Personally 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.

³Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, testimony delivered on February 26, 2015.

⁴GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 2015).

⁵See GAO, *High-Risk Series: An Overview*, [GAO/HR-97-1](#) (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: January 2003).

⁶See [GAO-15-290](#).

⁷The *Federal Information Security Management Act of 2002* was enacted as Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

OMB, selected congressional committees, and the Comptroller General and are to address the adequacy of information security policies, procedures, practices, and compliance with requirements. The act also included a provision for GAO to periodically report to Congress on agency implementation of the act's provisions. FISMA 2002 was updated in 2014 by the *Federal Information Security Modernization Act of 2014*.⁸ Because FISMA 2002 requirements were in effect during the time period of our review, we are evaluating agencies' implementation of those requirements in this report. We will refer to the 2002 law as FISMA 2002 and the *Federal Information Security Modernization Act of 2014* as FISMA 2014. Changes in information security requirements under FISMA 2014 are discussed later in this section.

Our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agencies' implementation of FISMA 2002 requirements. To do this, we reviewed and analyzed the provisions of FISMA 2002 to identify responsibilities for implementing, overseeing, and providing guidance for agency information security. We also compared requirements for FISMA 2002 against those in FISMA 2014 to identify revised roles and responsibilities for OMB, the Department of Homeland Security (DHS), and federal agencies. We also analyzed our previous information security reports, annual agency FISMA reports, and agency financial and performance and accountability reports from the 24 federal agencies covered by the *Chief Financial Officers Act*,⁹ reports from the 24 agencies' Offices of Inspector General, OMB's annual reports to Congress on FISMA 2002 implementation, and NIST security publications issued for or during fiscal years 2013 and 2014. Where possible, we

⁸The *Federal Information Security Modernization Act of 2014* was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code. FISMA 2014 largely supersedes the very similar FISMA 2002 and expands the role and responsibilities of the Department of Homeland Security, but retains many of the requirements for federal agencies' information security programs previously set by the 2002 law.

⁹The 24 *Chief Financial Officers Act* agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

categorized findings from those reports according to information security program requirements prescribed by FISMA 2002 and security control areas defined by our *Federal Information System Controls Audit Manual*.¹⁰ We also reviewed OMB and DHS' annual FISMA reporting guidance and OMB's annual reports to Congress for fiscal years 2013 and 2014 FISMA implementation. In addition, we analyzed, categorized, and summarized the annual FISMA data submissions for fiscal years 2013 and 2014 by each agency's chief information officer, inspector general, and senior agency official for privacy.¹¹ We selected six agencies to determine the reliability of agency-submitted data. These agencies were selected to reflect a range in the number of systems agencies reported in fiscal year 2013 and include the Departments of Commerce, State, and Treasury; the General Services Administration; the National Science Foundation; and the Social Security Administration. While not generalizable to all agencies, the information we collected and analyzed provided insights into various processes in place to produce FISMA reports. We also conducted interviews with agency officials at OMB, DHS, NIST, and the six selected agencies. For the six agencies, we collected data from inspectors general and agency officials. Based on this assessment, we determined that the data were sufficiently reliable for our work.

We conducted this performance audit from December 2014 to September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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. For more details on our objectives, scope, and methodology, see appendix I.

Background

To help protect against threats to federal systems, FISMA 2002 set forth a comprehensive framework for ensuring the effectiveness of information

¹⁰GAO, *Federal Information System Controls Audit Manual (FISCAM)*, [GAO-09-232G](#) (Washington, D.C.: February 2009).

¹¹The inspectors general data submissions and OMB's report to Congress did not include information on recommendations that were made to address weaknesses discussed and any actions taken.

security controls over information resources that support federal operations and assets. This framework created a cycle of risk management activities necessary for an effective security program. It was also intended to provide a mechanism for improved oversight of federal agency information security programs. To ensure the implementation of this framework, FISMA 2002 assigned specific responsibilities to agencies, their inspectors general, OMB, and NIST.

FISMA 2002 required each agency in the executive branch to develop, document, and implement an information security program that includes the following components:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- subordinate plans for providing adequate information security for networks, facilities, and systems or a group of information systems, as appropriate;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and

-
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, each of the agencies in the executive branch were to report annually to OMB, certain congressional committees, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and their compliance with the act. FISMA 2002 also required each agency inspector general, or other independent auditor, to annually evaluate and report on the information security program and practices of the agency.

OMB's responsibilities included developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in federal agencies except with regard to national security systems.¹² FISMA 2002 also assigned responsibility to OMB for ensuring the operation of a federal information security incident center. The required functions of this center are performed by DHS's United States Computer Emergency Readiness Team (US-CERT), which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. OMB is also responsible for reviewing, at least annually, and approving or disapproving agencies' information security programs.

Since it began issuing guidance to agencies in 2003, OMB has instructed agency chief information officers and inspectors general to report on a variety of metrics in order to satisfy reporting requirements established by FISMA 2002. Over time, these metrics have evolved to include administration priorities and baseline metrics meant to allow for measurement of agency progress in implementing information security-related priorities and controls. OMB requires agencies and inspectors

¹²As defined in FISMA 2002 and FISMA 2014, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3552(b)(6).

general to use an interactive data collection tool called CyberScope¹³ to respond to these metrics. The metrics are used by OMB to summarize agencies' progress in meeting FISMA 2002 requirements and report this progress to Congress in an annual report, as required by FISMA 2002.

NIST's responsibilities under FISMA 2002 included the development of security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of impact-levels (See Federal Information Processing Standards 199 and 200),¹⁴ minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.

During the 12 years FISMA 2002 was enacted into law and then largely replaced by FISMA 2014, executive branch oversight of agency information security has evolved. As part of its FISMA 2002 oversight responsibilities, OMB has issued annual instructions for agencies and inspectors general to meet FISMA 2002 reporting requirements. In July 2010, the Director of OMB and the White House Cybersecurity Coordinator issued a joint memorandum¹⁵ that gave DHS primary responsibility within the executive branch for the operational aspects of cybersecurity for federal information systems that fall within the scope of FISMA 2002. This memo stated that DHS would have these five responsibilities:

- overseeing implementation of and reporting on government cybersecurity policies and guidance;
- overseeing and assisting government efforts to provide adequate, risk-based, and cost-effective cybersecurity;

¹³CyberScope is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a federal agency's information infrastructure. Agencies are required to use this tool to report metrics.

¹⁴NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004) and NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

¹⁵OMB, *Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C.: July 6, 2010).

-
- overseeing agencies' compliance with FISMA 2002;
 - overseeing agencies' cybersecurity operations and incident response; and
 - annually reviewing agencies' cybersecurity programs.

The OMB memo further stated that, in carrying out these responsibilities, DHS was to be subject to general OMB oversight in accordance with the provisions of FISMA 2002. In addition, the Cybersecurity Coordinator would lead the interagency process for cybersecurity strategy and policy development.

In accordance with guidance contained in the memo, DHS, instead of OMB, issued guidance to agencies and inspectors general on metrics used for reporting agency performance of cybersecurity activities and privacy requirements, while OMB continued to provide more general reporting guidance.¹⁶ Specifically, DHS provided guidance to agencies for reporting on the implementation of security requirements in areas such as continuous monitoring, configuration management, incident response, security training, and contingency planning, among others. The guidance also instructs inspectors general on reporting the results of their annual evaluations and instructs senior agency officials for privacy on reporting their agencies' implementation of privacy requirements.

As previously mentioned, DHS is also responsible for ensuring the operation of a federal information security incident center to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. Within DHS, the Federal Network Resilience division's Cybersecurity Performance Management Branch is responsible for (1) developing and disseminating FISMA 2002 reporting metrics, (2) managing the CyberScope web-based application, and (3) collecting and reviewing federal agencies' cybersecurity data submissions and monthly data feeds to CyberScope. In addition, the Cybersecurity Assurance Program Branch is responsible for conducting cybersecurity reviews and

¹⁶Fiscal year 2013 reporting instructions for FISMA and agency privacy management were issued by DHS as *Federal Information Security Memorandum 13-01* (Sept. 4, 2013) and by OMB as M-14-04 (Nov. 18, 2013). Fiscal year 2014 reporting instructions were issued by DHS as *Federal Information Security Memorandum 14-01* (undated memo) and by OMB as M-15-01 (Oct. 3, 2014). The DHS and OMB memos vary in content.

assessments at federal agencies to evaluate the effectiveness of agencies' information security programs.

New FISMA Requirements Clarify Roles and Responsibilities

To further improve cybersecurity and clarify oversight responsibilities, Congress passed FISMA 2014.¹⁷ FISMA 2014 is intended to address the increasing sophistication of cybersecurity attacks, promote the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provide for improved oversight of federal agencies' information security programs. Specifically, the act clarifies and assigns additional responsibilities to OMB, DHS, and federal agencies in the executive branch. These new responsibilities include:

OMB responsibilities

- Preserves OMB's oversight responsibilities, but removes the requirement for OMB to annually review and approve agencies' information security programs.
- Requires OMB to include in its annual report to Congress a summary of major agency information security incidents, an assessment of agency compliance with NIST standards, and an assessment of agency compliance with breach notification requirements. For two years after enactment, OMB is to include in its annual report an assessment of agencies' adoption of continuous diagnostic technologies and other advanced security tools.
- Requires OMB to update data breach notification policies and guidelines periodically and require notice to congressional committees and affected individuals.
- Expands exemptions from OMB oversight for certain national security-related systems.
- States that OMB shall, in consultation with DHS, the Chief Information Officers Council, the Council of Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

¹⁷Note: This report covers agencies' fiscal years 2013 and 2014 efforts under the requirements of FISMA 2002.

DHS responsibilities

- Establishes DHS responsibility, in consultation with OMB, to administer the implementation of agency information security policies and practices for information systems other than national security systems, the Department of Defense, and the Intelligence community's "debilitating impact" systems.
- Requires DHS to develop, issue, and oversee implementation of binding operational directives to agencies. Such directives include those for incident reporting, contents of annual agency reports, and other operational requirements.
- Gives DHS responsibility to operate the federal information security incident center, deploy technology to continuously diagnose and mitigate threats, compile and analyze data, and develop and conduct targeted operational evaluations, including threat and vulnerability assessments of systems.

Executive branch agency responsibilities

- Requires agencies to comply with DHS operational directives in addition to OMB policies and procedures and NIST standards.
- Requires agencies to ensure that senior officials carry out assigned responsibilities and that all personnel are held accountable for complying with the agency's information security program.
- Requires agencies to use automated tools in periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices.
- Requires agencies to report major security incidents to Congress within 7 days. Agencies are also to include a description of major incidents in their annual report to Congress.
- FISMA 2014 also requires that the annual independent evaluation include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. This replaces the previous FISMA 2002 requirement that the independent annual evaluation include an assessment of agency compliance with the requirements of the act and related policies, procedures, standards, and guidelines.

In addition, FISMA 2014 reiterates the previous requirement for federal agencies to develop, document, and implement an agency-wide information security program. Each agency and its Office of Inspector General are still required to report annually to OMB, selected

congressional committees, and the Comptroller General on the adequacy of the agency's information security policies, procedures, practices, and compliance with requirements.

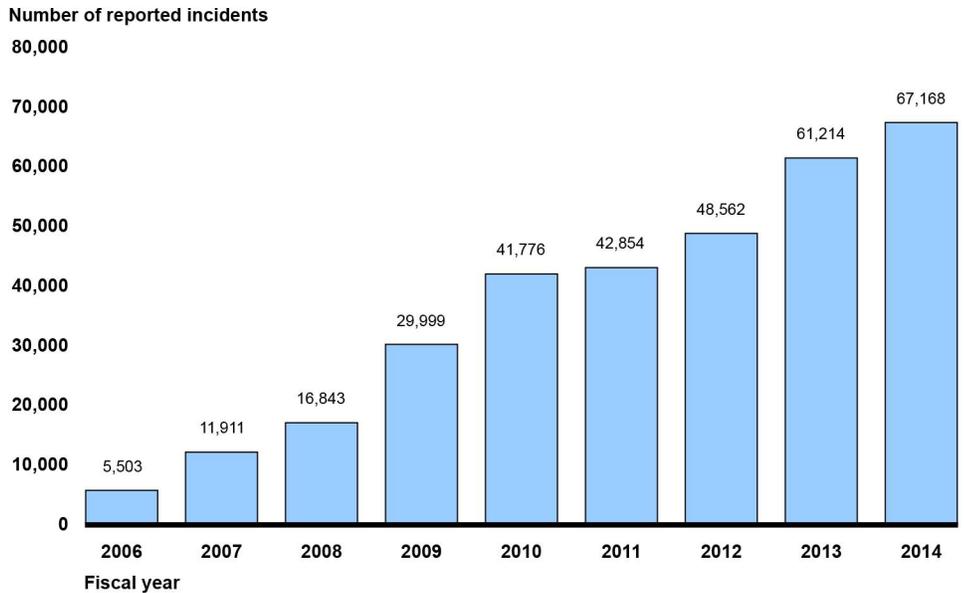
Continued Weaknesses Place Federal Agencies' Information and Information Systems at Risk

During fiscal years 2013 and 2014, federal agencies continued to experience weaknesses in protecting their information and information systems. These systems remain at risk as illustrated in part by the evolving array of cyber-based threats and the increasing numbers of incidents reported by federal agencies. (See app. II for additional information on cyber threats and exploits.) At the same time, weaknesses in their information security policies and practices hinder their efforts to protect against threats. Furthermore, our work and reviews by inspectors general highlight information security control deficiencies at agencies that expose information and information systems supporting federal operations and assets to elevated risk of unauthorized use, disclosure, modification, and disruption. Accordingly, we and agency inspectors general have made hundreds of recommendations to agencies to address these security control deficiencies.

Number of Incidents Reported by Federal Agencies Continues to Increase

The number of information security incidents affecting systems supporting the federal government has continued to increase. Since fiscal year 2006, the number rose from 5,503 to 67,168 in fiscal year 2014: an increase of 1,121 percent. Figure 1 illustrates the increasing number of security incidents at federal agencies from 2006 through 2014.

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



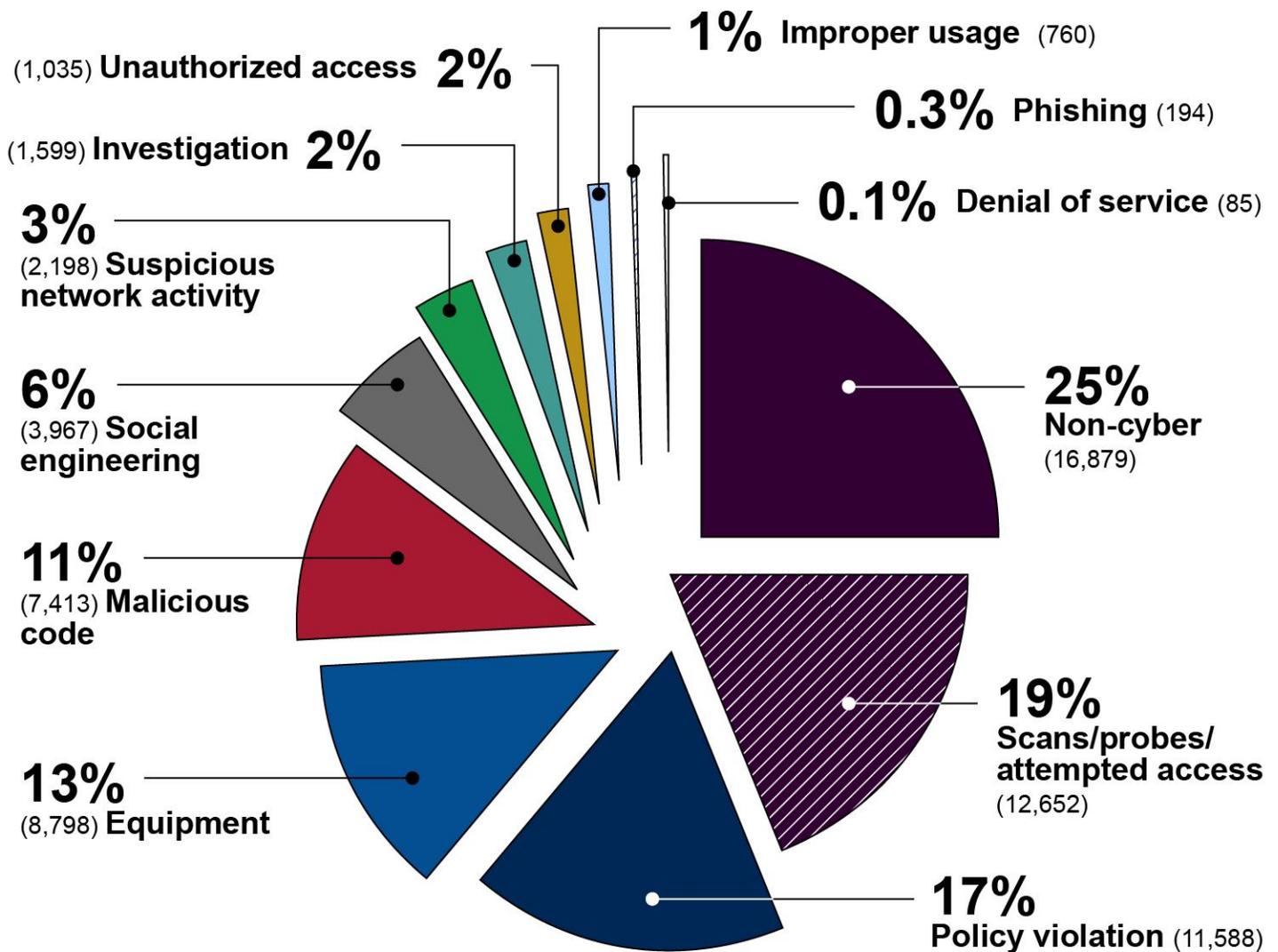
Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-714

Similarly, the number of information security incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Of the incidents occurring in 2014 (not including those reported as non-cyber incidents)¹⁸ scans/probes/attempted access was the most widely reported type of incident across the federal government. This type of incident can involve identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. As shown in figure 2, these incidents represented 19 percent of the various incidents reported to US-CERT in fiscal year 2014.

¹⁸A non-cyber incident is a report of PII spillage or possible mishandling of PII that involves hard copies or printed material as opposed to digital records.

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



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-714

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. Recent examples highlight the impact of such incidents:

- In June 2015, OPM reported that an intrusion into its systems affected the personnel records of about 4.2 million current and former federal employees. The Director of OPM also stated that a separate but

related incident affected background investigation files and compromised OPM systems related to background investigations 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. These data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the Internal Revenue Service 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.¹⁹
- 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.²⁰
- 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.²¹

¹⁹Department 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).

²⁰James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Committee on Armed Services, Feb. 26, 2015.

²¹Randy 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, Nov. 19, 2014.

-
- 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.²²

Cybersecurity Deficiencies Continue to Place Systems at Risk

Our work at federal agencies continues to highlight information security deficiencies in both financial and nonfinancial systems. We have made hundreds of recommendations to agencies to address these security control deficiencies, but many have not yet been fully implemented. The following examples describe the risks we found at federal agencies, our recommendations, and the agencies' responses to our recommended actions.

- In March 2015, we reported that the Internal Revenue Service had not installed appropriate security updates on all of its databases and servers, and had not sufficiently monitored control activities that support its financial reporting and protect taxpayer data. Also, the agency had not effectively maintained secure settings or separation of duties by allowing a developer unnecessary access to a key application. In addition to 51 recommendations made in prior years that remain unimplemented, we made 19 additional recommendations to help the agency more effectively implement elements of its information security program and address newly identified control weaknesses. The Internal Revenue Service agreed to develop corrective action plans, as appropriate, to address these recommendations.²³
- In January 2015, we reported that the Federal Aviation Administration had significant security control weaknesses in the five air traffic control systems we reviewed. These systems perform functions such as determining and sharing precise aircraft location, streaming flight information to cockpits of aircraft, providing telecommunications infrastructure for NextGen, and are necessary for ensuring the safe and uninterrupted operation of the national airspace system. We identified numerous weaknesses in controls intended to prevent, limit,

²²Department 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).

²³GAO, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*, [GAO-15-337](#) (Washington D.C.: March 19, 2015).

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 its systems. The agency also had not fully implemented an agency-wide information security program, in part due to not having fully established an integrated, organization-wide approach to managing information security risk. We made 168 recommendations to the agency to mitigate control deficiencies and 17 recommendations to fully implement its information security program and establish an integrated approach to managing information security risk. The Federal Aviation Administration concurred with our recommendations, described actions that it was taking to improve its information security, and indicated that it would address the recommendations.²⁴

- In November 2014, we reported that the Department of Veterans Affairs had not taken effective actions to contain and eradicate a significant incident detected in 2012 involving a network intrusion. Further, the department's actions to address vulnerabilities identified in two key web applications were insufficient. Additionally, vulnerabilities identified in workstations (e.g., laptop computers) had not been corrected. We made eight recommendations to address identified weaknesses in incident response, web applications, and patch management. The department concurred with our recommendations and provided an action plan for addressing the identified weaknesses.²⁵

Similar to our work, 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 reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their

²⁴GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, [GAO-15-221](#) (Washington D.C.: Jan. 29, 2015).

²⁵GAO, *Information Security: VA Needs to Address identified Vulnerabilities*, [GAO-15-117](#) (Washington D.C.: Nov. 13, 2014).

financial reporting.²⁶ This reflected an increase from fiscal year 2013, when 18 agencies reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting. Further, 23 of 24 inspectors general for the agencies cited information security as a “major management challenge” for their agency, reflecting an increase from fiscal year 2013, when 21 inspectors general cited information security as a major challenge. The inspectors general made numerous recommendations to address these issues, as discussed later in this report.

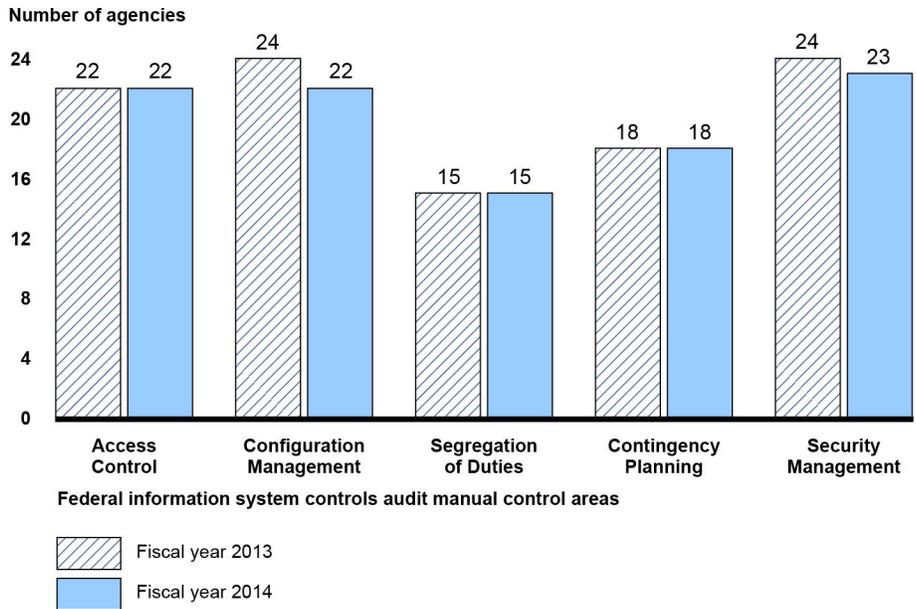
Agencies Exhibited Weaknesses in All Major Categories of Controls

Our reports, agency reports, and inspectors general assessments of information security controls during fiscal years 2013 and 2014 revealed that most of the 24 agencies had weaknesses in each of the five major categories of information system controls: (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, which helps avoid significant disruptions in computer-dependent operations; and (5) agencywide security management, which provides a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended.

While the number of agencies exhibiting weaknesses decreased slightly in two of five categories, deficiencies were prevalent for the majority of them, as shown in figure 3.

²⁶A “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.

Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014



Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

In the following subsections, we discuss the specific information security weaknesses agencies reported for fiscal years 2013 and 2014.

Most Agencies Had Weaknesses in Access Controls

Agencies use electronic and physical controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized use, modification, disclosure, and loss. Access controls involve the six critical elements described in table 1.

Table 1: Critical Elements for Access Control to Computer Resources

Element	Description
Boundary protection	Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices that are connected to a network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection and prevention technologies can be deployed to defend against attacks from the Internet.
User identification and authentication	A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns a unique user account to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication provides the basis for establishing accountability and for controlling access to the system.
Authorization	Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have some built-in authorization features such as permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device.
Cryptography	Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Examples of cryptographic services are encryption, authentication, digital signature, and key management. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information.
Auditing and Monitoring	To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is necessary to determine what, when, and by whom specific actions have been taken on a system. Agencies do so by implementing software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities.
Physical Security	Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources. Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas is to be managed appropriately.

Source: GAO | GAO-15-714

For fiscal years 2013 and 2014, we, agencies, and inspectors general reported weaknesses in access controls for 22 of the 24 agencies. In fiscal year 2014, 12 agencies had weaknesses reported in protecting their networks and system boundaries, a reduction from the 17 agencies that had weaknesses in fiscal year 2013. For example, we found that 1 agency component's access control lists on a firewall had not prevented traffic coming or initiated from the public internet protocol addresses of a

contractor site and a U.S. telecom corporation from entering to its network. Additionally, for fiscal year 2014, 20 agencies had weaknesses reported in their ability to appropriately identify and authenticate system users, a slight increase from 19 of 24 in fiscal year 2013. To illustrate, in fiscal year 2014, 1 agency had not consistently applied proper password settings to mainframe service accounts, where those accounts were configured to never require password changes. Agencies also had weak password controls, such as using system passwords that had not been changed from the easily guessable default passwords.

In fiscal year 2014, 18 agencies had weaknesses reported in authorization controls, a reduction from the 20 agencies that had weaknesses in fiscal year 2013. One example of this weakness for fiscal year 2014 was that 1 agency had not consistently or in a timely manner removed, transferred, and/or terminated employee and contractor access privileges from multiple systems. Another agency had granted access privileges unnecessarily, which allowed users of an internal network to read and write files containing sensitive system information, including passwords, that were used to support automated data transfer operations between numerous systems. In fiscal year 2014, 4 agencies had weaknesses reported in encryption, down from 7 in fiscal year 2013.

In addition, 19 agencies had weaknesses reported in implementing an effective audit and monitoring capability. For instance, 1 agency had not effectively implemented audit and monitoring controls on a system where the servers and network devices were not sufficiently logging security-relevant events. Finally, 10 agencies had weaknesses reported in their ability to restrict physical access or harm to computer resources and protect them from unauthorized loss or impairment. For example, a contractor of an agency was granted physical access to a server room without the required approval of the office director. Without adequate access controls in place, agencies cannot ensure that their information resources are being protected from intentional or unintentional harm.

Agencies Did Not Fully Implement Controls for Configuration Management

Configuration management controls 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. These controls, which limit and monitor access to powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls and the operations of systems and networks are not compromised. To protect against known vulnerabilities, effective

procedures must be in place, current versions of vendor-supported software installed, and patches promptly implemented. Up-to-date patch installation helps mitigate known flaws in software code that could be exploited to cause significant damage and enable malicious individuals to read, modify, or delete sensitive information or disrupt operations.

In fiscal year 2014, 22 agencies had weaknesses reported in configuration management, a reduction from the 24 agencies that had weaknesses in fiscal year 2013. For fiscal year 2014, 17 agencies had weaknesses reported with installing software patches and implementing current versions of software in a timely manner, an improvement from the 23 reported in fiscal year 2013. One agency had not installed critical updates in a timely manner for several of its servers. Another agency was using an unsupported software application on its workstations, and a database system used to support the access authorization system was no longer supported. For fiscal year 2014, 14 agencies had weaknesses reported in authorizing, testing, approving, tracking, and controlling configuration changes. In fiscal year 2014, our work revealed that 1 agency had not effectively documented and approved configuration changes. Specifically, the agency did not request or approve 32 changes to mainframe production processing that had been recorded in the system logs.

Without a consistent approach to testing, updating, and patching software, agencies increase their risk of exposing sensitive data to unauthorized and possibly undetected access.

More than Half of the Agencies Did Not Segregate Incompatible Duties

Segregation of duties refers to 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. Key steps to achieving proper segregation are ensuring that incompatible duties are separated and employees understand their responsibilities, and controlling personnel activities through formal operating procedures, supervision, and review.

In fiscal years 2013 and 2014, 15 agencies had weaknesses reported in implementing segregation of duties controls. For example, in fiscal year 2014, 1 agency had not implemented requirements for separating incompatible duties. Additionally, a developer from another agency had been authorized inappropriate access to the production environment of the agency's system. Further, another agency had not adequately implemented segregation of duties controls for IT and financial

management personnel with access to financial systems across several platforms and environments.

Without adequate segregation of duties, agencies increase the risk that erroneous or fraudulent actions will occur, improper program changes will be implemented, and computer resources will be damaged or destroyed.

Agencies Had Weaknesses in Continuity of Operations

In the event of an act of nature, fire, accident, sabotage, or other disruption, an essential element in preparing for the loss of operational capabilities is having an up-to-date, detailed, and fully tested continuity of operations plan. This plan should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing it and making necessary adjustments. If continuity of operations controls are faulty, even relatively minor interruptions can result in lost or incorrectly processed data, which can lead to financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.

Eighteen agencies had weaknesses reported in continuity of operations practices for their agencies in fiscal years 2014 and 2013. Specifically, in 2014, 16 agencies did not have a comprehensive contingency plan. For example, 1 agency's contingency plans had not been updated to reflect changes in the system boundaries, roles and responsibilities, and lessons learned from testing contingency plans at alternate processing and storage sites. Additionally, 15 agencies had not regularly tested their contingency plans. For example, 1 agency had not annually tested contingency plans for 10 of its 16 systems.

Until agencies address identified weaknesses in their continuity of operations plans and tests of these plans, they may not be able to recover their systems in a successful and timely manner when service disruptions occur.

Agencies Did Not Effectively Manage Security

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented an agency-wide information security program to help them manage their security process. An agency-wide security program, as required by FISMA 2002, 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. Without a well-

We and Inspectors General
Recommended Actions to
Strengthen Information
Security

designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

In fiscal year 2014, 23 agencies had weaknesses reported in security management, while 24 had them in fiscal year 2013. In one example, an agency had not fully developed and implemented components of its agency-wide information security risk management program that met FISMA's requirements. Specifically, the agency had established an enterprise risk management framework; however, security risks had not been fully communicated to data centers, regional offices, and medical facilities. In another example, the agency did not have effective procedures for testing and evaluating controls since the procedures did not prescribe effective tests of authentication controls.

Until agencies fully resolve identified deficiencies in their agency-wide information security programs, they will continue to face significant challenges in protecting their information and systems.

Over the last several years, we and agency inspectors general have made hundreds of 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 and inspectors general 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. 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 Underway to Improve Security

Due to the increase in cyber security threats, the federal government has initiated or continued several efforts to protect federal information and information systems. The White House, OMB, and federal agencies have launched several government-wide efforts that are intended to enhance information security at federal agencies. These key efforts are discussed here.

Cybersecurity Cross-Agency Priority goals: Initiated in 2012, the cybersecurity Cross-Agency Priority (CAP) goals are an effort intended to focus federal agencies' cybersecurity activity on the most effective controls. For fiscal years 2013 and 2014, these goals included:

- **Trusted Internet Connections:** 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 fiscal year 2014 targets of 95 percent for TIC consolidation and 100 percent for implementing TIC capabilities. OMB reported that agencies had achieved 95 and 92 percent implementation, respectively, for these TIC goals in fiscal year 2014.
- **Continuous monitoring:** 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 implementation for continuous monitoring and reported that the agencies had achieved 92 percent implementation.
- **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. OMB established a fiscal year 2014 target of 75 percent implementation for strong authentication. In its report on fiscal year 2014 FISMA implementation, OMB indicated that the 24 federal agencies covered by the CFO Act had achieved a combined 72 percent implementation of these requirements, but this

number dropped to only 41 percent implementation for the 23 civilian agencies when excluding DOD.²⁷

In fiscal year 2015, the administration added the anti-phishing and malware defense as a new goal for the CAP initiative.

The National Cybersecurity Protection System (NCPS): NCPS is a system of systems (also known as EINSTEIN) 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. This system was created in 2003 by US-CERT to help reduce and prevent computer network vulnerabilities across the federal government. The capabilities of NCPS are to include network “flow,” intrusion detection, and intrusion prevention functions, as described in table 2.²⁸

²⁷Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Washington D.C.: Feb. 27, 2015).

²⁸The Senate and House reports accompanying the *Consolidated Appropriations Act, 2014* included a provision for us to review NCPS. 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.

Table 2: National Cybersecurity Protection System Capabilities

Operational name	Capability provided	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. [Note A]
EINSTEIN 2	Intrusion detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts the United States Computer Emergency Readiness Team (US-CERT) when specific network activity matching the predetermined signatures has been detected. [Note B]
EINSTEIN 3	Intrusion prevention	Automatically blocks malicious traffic from entering or leaving 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. [Note C]

Source: GAO analysis of DHS documentation and prior GAO reports. | GAO-15-714

Note 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.

Note B: Signatures are recognizable, distinguishing patterns associated with a cyber attack, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

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

The Continuous Diagnostics and Mitigation (CDM) Program: CDM is intended to provide federal departments and agencies with a basic set of tools to support the continuous monitoring of information systems. According to DHS, the 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 acquisition vehicle to allow federal agencies (as well as state, local, and tribal governmental agencies) to acquire CDM tools at discounted rates.

The National Initiative for Cybersecurity Education (NICE): NICE is an interagency effort coordinated by NIST to improve cybersecurity education, including efforts directed at training, public awareness, and the federal cybersecurity workforce. This initiative is intended to support the

federal government's evolving strategy for education, awareness, and workforce planning and provide a comprehensive cybersecurity education program. To meet NICE objectives, efforts were structured into the following four components:

1. **National cybersecurity awareness:** This component included public service campaigns to promote cybersecurity and responsible use of the Internet and to make cybersecurity popular for children. It was also aimed at making cybersecurity a popular educational and career pursuit for older students.
2. **Formal cybersecurity education:** Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity were included in this component, which focused on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for private sector and government.
3. **Federal cybersecurity workforce structure:** This component addressed personnel management functions, including the definition of cybersecurity jobs in the federal government and the skills and competencies they required. Also included were new strategies to ensure federal agencies can attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
4. **Cybersecurity workforce training and professional development:** Cybersecurity training and professional development for federal government civilian, military, and contractor personnel were included in this component.

The Federal Risk and Authorization Management Program

(FedRAMP): FedRAMP is a government-wide program intended to provide a standardized approach to security assessment, authorization,²⁹ and continuous monitoring for cloud computing products and services.³⁰

²⁹Security authorization is the official management decision given by a senior official of an organization to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation, based on the implementation of an agreed-on set of security controls.

³⁰FedRAMP's security assessment framework encompasses four process areas (document, assess, authorize, and monitor) that are based on the six steps within the framework described in NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

FedRAMP defines a set of controls for low and moderate impact-level systems according to the baseline controls in NIST SP 800-53 Revision 4³¹ and includes control enhancements related to the unique security requirements of cloud computing. All federal agencies must meet FedRAMP requirements when using cloud services and the cloud service providers must implement the FedRAMP security requirements in their cloud environment.

In addition, the cloud service providers must hire a FedRAMP-approved third-party assessment organization to perform an independent assessment to audit the cloud system and provide a security assessment package for review. The package will then be reviewed by the FedRAMP Joint Authorization Board,³² which may grant a provisional authorization. Federal agencies can leverage cloud service provider authorization packages for review when granting an agency authority to operate, where this reuse is intended to save time and money. After the cloud provider has received a FedRAMP authorization from the Joint Authorization Board or the agency, it must implement a continuous monitoring capability to ensure the cloud system maintains an acceptable risk posture.

The Cyber and National Security Team (E-Gov Cyber): OMB created the Cyber and National Security Team, called the E-Gov Cyber Unit, to strengthen federal cybersecurity through targeted oversight and policy issuance. The unit and its partners, the National Security Council, DHS, and NIST, are to oversee agency and government-wide cybersecurity programs, and oversee and coordinate the federal response to major cyber incidents and vulnerabilities. OMB reported that the unit found that more than half of incidents occurring at federal agencies could have been prevented by strong authentication. In addition, the unit intends to monitor implementation of critical DHS programs such as NCPs and CDM.

The 30-Day Cybersecurity Sprint: In June 2015, in response to the OPM security breaches and to improve federal cybersecurity and protect

³¹NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

³²The Joint Authorization Board is composed of the chief information officers from DOD, DHS, and the General Services Administration and establishes the baseline controls for FedRAMP and criteria for accrediting third-party independent assessment organizations.

systems against evolving threats, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint. As part of this effort, the Federal Chief Information Officer instructed federal agencies to immediately take a number of steps to further protect federal information and assets and to improve the resilience of federal networks. Specifically, federal agencies were to:

- Immediately deploy indicators provided by DHS regarding priority threat actor techniques, tactics, and procedures to scan systems and check logs. Agencies were to inform DHS immediately if indicators return evidence of malicious cyber activity.
- Patch critical vulnerabilities without delay. The vast majority of cyber intrusions exploit well-known vulnerabilities that are easy to identify and correct. Agencies were to take immediate action on the DHS vulnerability scan reports they receive each week and report to OMB and DHS on progress and challenges within 30 days.
- Tighten policies and practices for privileged users. To the greatest extent possible, agencies were to minimize the number of privileged users; limit functions that can be performed when using privileged accounts; limit the duration that privileged users can be logged in; limit the privileged functions that can be performed using remote access; and ensure that privileged user activities are logged and that such logs are reviewed regularly. Agencies were to report to OMB and DHS on progress and challenges within 30 days.
- Dramatically accelerate implementation of multi-factor authentication, especially for privileged users. Intruders can easily steal or guess usernames/passwords and use them to gain access to federal networks, systems, and data. Requiring the use of a personal identity verification card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating federal networks and systems. Agencies were to report to OMB and DHS on progress and challenges in implementation of these enhanced security requirements within 30 days.
- In addition to providing guidance to the agencies, the Federal Chief Information Officer established the Cybersecurity Sprint Team to lead a review of the federal government's cybersecurity policies, procedures, and practices. According to OMB, the team is comprised of OMB's E-Gov Cyber and National Security Unit, the National Security Council Cybersecurity Directorate, DHS, and DOD. At the end of the review, the Federal Chief Information Officer is to create

and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a federal civilian cybersecurity strategy. Key principles of the strategy are to include:

- **Protecting data:** Better protect data at rest and in transit.
- **Improving situational awareness:** Improve indication and warning.
- **Increasing cybersecurity proficiency:** Ensure a robust capacity to recruit and retain cybersecurity personnel.
- **Increasing awareness:** Improve overall risk awareness by all users.
- **Standardizing and automating processes:** Decrease time needed to manage configurations and patch vulnerabilities.
- **Controlling, containing, and recovering from incidents:** Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
- **Strengthening systems Life-cycle security:** Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
- **Reducing attack surfaces:** Decrease complexity and number of things defenders need to protect.

Successful implementation of these government-wide efforts will be key steps to improving cybersecurity at federal agencies.

Agencies' Implementation of FISMA 2002 Requirements Was Mixed

The extent of agencies' implementation of FISMA 2002 requirements for establishing and maintaining an information security program from fiscal year 2013 to fiscal year 2014 varied.³³ For example, according to the reports by the inspectors general of the 24 CFO Act agencies, the number of agencies implementing risk management activities and documenting policies and procedures increased while the number of agencies planning for security, providing security training, and testing controls decreased. In addition, agency inspectors general, NIST, and OMB, with support from DHS, continued to address their responsibilities under FISMA 2002, but opportunities remain for improving FISMA reporting.

More Agencies Implemented Risk Management Activities

FISMA 2002 required that agencies periodically assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. These risk assessments help determine whether controls are in place to remediate or mitigate risk to the agency. NIST has issued several guides for managing risk.³⁴

According to NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems*, risk management is addressed at the organization level, the mission and business process level, and the information system level. Risks are addressed from an organizational perspective with the development of, among other things, risk management policies, procedures, and strategy. The risk decisions made at the organizational level are to guide the entire risk management program. In addition, the activities for the risks that are addressed at the

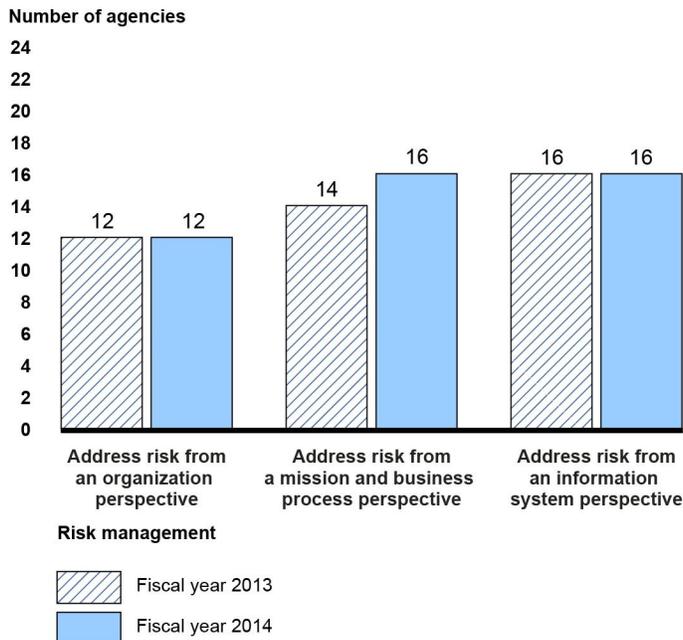
³³FISMA 2002 required that agencies implement security programs that included periodic assessments of risk; risk-based security policies and procedures; security training and awareness; periodic testing and evaluation of controls; a process for planning, implementing, evaluating, and documenting remedial actions; procedures for detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations, among other items. These requirements of FISMA 2002 are continued in FISMA 2014 at 44 U.S.C. § 3554(b).

³⁴NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39 (Gaithersburg, Md.: March 2011); *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1; and *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1 (Gaithersburg, Md.: September 2012).

mission and business process levels include, among other things, defining and prioritizing the agency’s mission and business processes and developing an organization-wide information protection strategy. There are various risk management activities for the risks that are addressed at the information system level, including categorizing organizational information systems, allocating security controls to organizational information systems, and managing the selection, implementation, assessment, authorization, and ongoing monitoring of security controls.

For fiscal years 2014 and 2013, inspectors general reported that 12 agencies had addressed risk from an organization perspective. In fiscal year 2014, inspectors general reported that 16 of 24 agencies had addressed risk from a mission or business perspective compared to 14 in fiscal year 2013. According to inspectors general, for fiscal years 2013 and 2014, 16 agencies had addressed risk from an information system perspective. Figure 4 shows examples of agencies’ implementation of risk management program elements for fiscal years 2013 and 2014.

Figure 4: Examples of Agencies’ Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014



Source: GAO analysis of inspectors general *Federal Information Security Management Act* reports for fiscal years 2013 and 2014. | GAO-15-714

However, work by the inspectors general revealed weaknesses in risk management. According to OMB, inspectors general at seven agencies reported that their agency did not have a risk management program in place. The inspector general for one agency reported that, although the agency had implemented a risk governance structure, it had not fully identified or mitigated the enterprise-wide risks with appropriate risk mitigation strategies. Another inspector general reported that its agency did not have a current risk assessment for three of the seven systems in the sample. Managing risk is the center of an effective information security program; without effective risk management, agencies may not be fully aware of the risks to essential computing resources and may not be able to make informed decisions about needed security protections.

Most Agencies Had Documented Policies and Procedures

FISMA 2002 required agencies to develop, document, and implement policies and procedures that

- are based on risk assessments;
- cost-effectively reduce information security risks to an acceptable level;
- ensure that information security is addressed throughout the life cycle of each agency's information system; and
- ensure compliance with FISMA 2002 requirements, OMB policies and procedures, minimally acceptable system configuration requirements, and any other applicable requirements.

In fiscal years 2014 and 2013, most agency inspectors general reported that their agency had documented policies and procedures that were consistent with federal guidelines and requirements. Specifically, the number of agencies that documented policies and procedures increased in 8 of 11 categories, and remained the same in 3 categories since one inspector general did not report on these. Table 3 summarizes agencies' performance for fiscal years 2013 and 2014.

Table 3: Number of Agencies Documenting Information Security Policies and Procedures for Fiscal Years 2013 and 2014

Number	FISMA reporting area	Policies and procedures in place during fiscal year 2013	Policies and procedures in place during fiscal year 2014
1	Risk management	18	20
2	Configuration management	22	23
3	Incident response and reporting	20	21
4	Security training	20	23
5	Remedial actions	21	23
6	Remote access management	16	18
7	Identify and access management	19	21
8	Continuous monitoring	17	21
9	Continuity of operations	22	21 [Note A]
10	Oversight of contractor systems	21	20 [Note A]
11	Security capital planning	21 [Note A]	21 [Note A]

Source: CyberScope submissions for fiscal years 2013 and 2014. | GAO-15-714

Note A: In the CyberScope submission, one inspector general did not report on these programs and only 23 agencies were included.

In our prior work, we have also identified weakness in agencies policies and procedures for information security. In fiscal year 2014, we reported that six agencies we reviewed had not fully developed comprehensive policies and procedures for incident response. For example, only two of the six selected agencies had fully implemented policies that addressed roles, responsibilities, and levels of authority for incident response.³⁵ Similarly, we reported that several agencies had not established policies and procedures to oversee or assess the security of contractor systems.³⁶ Further, we found that one agency component’s mainframe security policy did not address who can administer the security software configurations that control access to mainframe programs.³⁷ We

³⁵GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 24, 2014).

³⁶GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

³⁷GAO-15-337.

recommended that these agencies develop and update policies and procedures for these areas. The agencies generally concurred with our recommendations.³⁸

Until all agencies properly document and implement policies and procedures, they may not be able to effectively reduce risks to their information and information systems, and the information security practices that are driven by these policies and procedures may be applied inconsistently.

Number of Agencies with Sufficient Security Planning Decreased

FISMA 2002 required agencies' information security programs to include plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. According to NIST, the purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.³⁹ The first step in the system security planning process is to categorize the system based on the impact to agency operations, assets, and personnel should the confidentiality, integrity, and availability of the agency's information and information systems be compromised. This categorization is then used to determine the appropriate security controls needed for each system. Another key step is selecting a baseline of security controls for each system and documenting those controls in the security plan.

In addition, NIST recommends that the plan be reviewed and updated at least annually. According to NIST, the security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls. The package contains a security plan, security assessment report, and plan of action and milestones (POA&M). DHS's fiscal year 2014 reporting instructions request inspectors general to report on their agencies implementation of

³⁸[GAO-14-354](#), [GAO-14-612](#), and [GAO-15-337](#).

³⁹NIST, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication (SP) 800-18 Revision 1 (Gaithersburg, Md.: February 2006).

certain program attributes⁴⁰ such as whether (1) the agency has categorized information systems, (2) its security authorization package contained system security plan, security assessment report, POA&M, and accreditation boundaries, and (3) it has selected and implemented a tailored set of baseline security controls.

In fiscal year 2014, agency inspectors general at 18 agencies reported that their agency had categorized information systems in accordance with federal policies, a decrease from fiscal year 2013, in which 19 inspectors general reported that their agency had categorized their systems. In addition, fewer agencies selected an appropriately tailored set of baseline security controls. For instance, in fiscal year 2014, 15 inspectors general stated that their agency had appropriately selected a baseline of security controls, while 16 had reported for fiscal year 2013. In addition, in fiscal year 2014, 13 inspectors general reported that their agency had implemented a tailored set of baseline security controls, another decrease from fiscal year 2013, in which 14 agencies were reported for such controls.⁴¹

For fiscal year 2014, according to the inspectors general, 15 agencies had completed a security authorization package that contained a system security plan; 8 had not completed one; and 1 inspector general responded that the question was “not applicable.” This is a decrease from fiscal year 2013, where 17 agencies had included such a security authorization package. In addition, inspectors general at 11 agencies reported that their agency had not always completed or properly updated their security plan. For example, a component of 1 agency had not completed one or more key elements of its system security plan, such as defining the system’s accreditation boundary. Further, at another agency, five systems had been placed into production without a system security plan.

⁴⁰Attributes are additional questions in each of 11 areas as defined in DHS’ FISMA reporting guidance to inspectors general. The attributes support the inspector’s general assessment of his or her department’s information security programs in those areas (see table 3 for a list of areas).

⁴¹In fiscal year 2014, the Inspector General for Commerce reported “not applicable” in this area. According to OMB, the Inspector General’s FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. The FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems.

Until agencies appropriately develop and update their system security plans, officials will not be aware of system security requirements or whether controls are in place.

Number of Agencies Providing Sufficient Security Awareness Decreased and the Percentage of Personnel Receiving Specialized Training Decreased

FISMA 2002 required agencies to provide security awareness training to personnel, including contractors and other users of information systems that support the operations and assets of the agency. Training is intended to inform agency personnel of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA 2002 also requires agencies to train and oversee personnel who have significant information security responsibilities. Providing training to agency personnel is critical to securing information and systems because people are one of the weakest links when securing systems and networks.

For fiscal year 2014, fewer agencies reported that at least 90 percent of their users had received security awareness training. The chief information officers for 22 agencies reported that they had provided annual security awareness training to at least 90 percent or more of their network users, which was a decrease from fiscal year 2013, when all 24 agencies reported that they had provided such training. Agency inspectors general reported similar results. For fiscal year 2014, inspectors general for 20 agencies reported that their agency had established a security awareness and training program, which was a decrease from fiscal year 2013, in which 21 agencies had established one. Similarly, they reported that fewer agencies had identified and tracked the status of security awareness training. Specifically, inspectors general for 16 agencies reported that their agency had identified and tracked the status of security awareness training in fiscal year 2014, a decrease from fiscal year 2013, in which 19 agencies had identified and tracked such training.

For fiscal year 2014, the percentage of personnel with significant security responsibilities who received training decreased from the previous year. In February 2015, OMB reported that, for fiscal year 2014, the 24 agencies provided training to an average of 80 percent of personnel who have significant security responsibilities, which reflects a decrease from the 92 percent reported for fiscal year 2013.

Without effective security awareness training, agency personnel may not have a basic understanding of information security requirements to protect the systems they use. In addition, personnel who did not take

specialized training may lack the knowledge, skills, and abilities consistent with their roles to protect the confidentiality, integrity, and availability of the information housed within the information systems to which they are assigned.

Fewer Agencies Are Periodically Testing and Continuously Monitoring Controls

FISMA 2002 required that federal agencies periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of implementing an agency-wide security program. This testing is to be performed with a frequency depending on risk, but no less than annually. Testing should include management, operational, and technical controls for every system identified in the agency's required inventory of major systems. This type of oversight is a fundamental element that demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results are used to improve security.

For fiscal year 2014, inspectors general reported that fewer agencies had tested and evaluated security controls using appropriate assessment procedures to determine the extent to which the controls had been implemented correctly, operated as intended, and produced the desired outcome with respect to meeting the security requirements for the system. In fiscal year 2014, 16 inspectors general reported that their agency had assessed security controls, while 17 agencies had assessed such controls in fiscal year 2013.⁴²

As part of government-wide efforts to improve the testing of controls, agencies have begun steps to implement continuous monitoring of their systems. According to NIST, the goal of continuous monitoring is to transform the otherwise static test and evaluation process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation. NIST defines information system continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

⁴²The Commerce Inspector General reported "not applicable" in this area in fiscal year 2014.

decisions.⁴³ Since March 2012, continuous monitoring has also been designated as a cross-agency priority area for improving federal cybersecurity.

Although OMB reported overall increases in the 24 agencies' continuous monitoring (from 81 percent in fiscal year 2013 to 92 percent in fiscal year 2014) of controls, inspectors general reported that fewer agencies had continuously monitored controls for their systems. For example, for fiscal year 2014, 12 inspectors general stated that their agency had ensured information security controls were being monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting a security impact analysis of the associated changes, and reporting the security state of the system to designated organizational officials. This is a decrease from fiscal year 2013, when 14 agencies had monitored security controls on an ongoing basis.⁴⁴

If controls are not effectively tested or properly monitored, agencies will have less assurance that they have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency.

Increasing Number of Agencies are Generally Implementing Elements of a Remediation Program, but Weaknesses Remain

FISMA 2002 required agencies to plan, implement, evaluate, and document remedial actions to address any deficiencies in their information security policies, procedures, and practices. In addition, NIST guidance states that federal agencies should develop a POA&M for information systems to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.⁴⁵ Furthermore, the POA&M should identify, among other things, the resources required to accomplish the tasks, and scheduled

⁴³NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication 800-137 (Gaithersburg, Md.: September 2011).

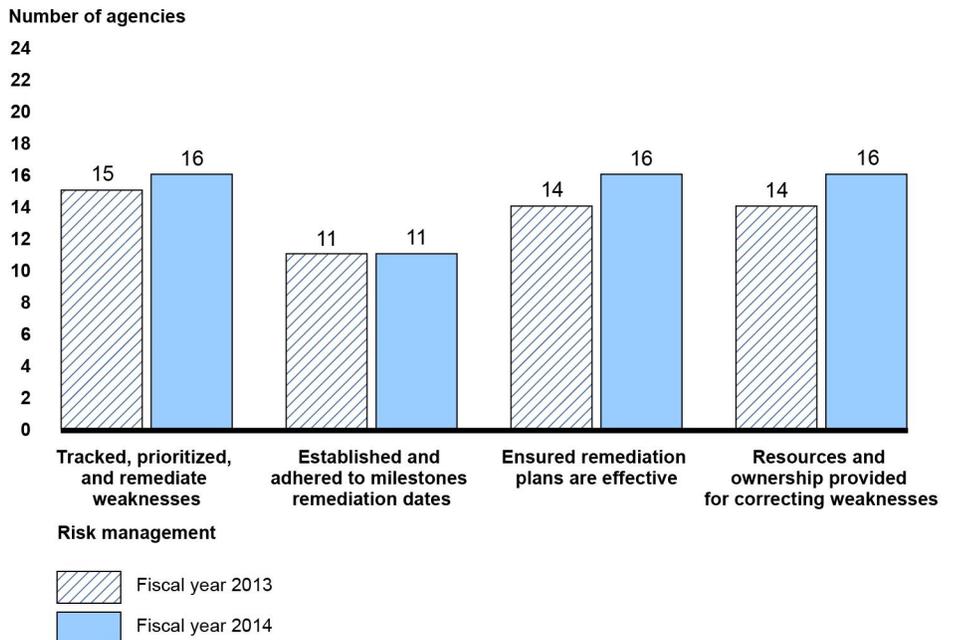
⁴⁴In fiscal year 2014, the Commerce Inspector General reported "not applicable" in this area.

⁴⁵NIST, Special Publication (SP) 800-53A, Revision 4 (Gaithersburg, Md.: December 2014).

completion dates for the milestones. According to OMB, remediation plans assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

For fiscal year 2014, the number of agencies implementing certain elements of their remediation programs increased or remained the same. For fiscal year 2014, inspectors general reported that 16 agencies had tracked, prioritized, and remediated weaknesses, compared to 15 for fiscal year 2013. In addition, 11 agencies had established and adhered to milestone remediation dates in both fiscal years. Further, 16 agencies were reported having an effective remedial action plan in fiscal year 2014, an increase from fiscal year 2013, in which 14 reported having such a plan. For fiscal year 2014, 16 inspectors general reported that their agency had ensured resources and ownership were provided for correcting weaknesses, which is also an increase from 14 in fiscal year 2013. Figure 5 shows agencies' remediation program efforts for fiscal years 2013 to 2014.

Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014



Source: GAO analysis of inspectors general *Federal Information Security Management Act* reports for fiscal years 2013 and 2014. | GAO-15-714

In spite of these increases, inspectors general reported, that for fiscal year 2014, 19 agencies had established a remediation program, which was a slight decrease from fiscal year 2013, in which 20 inspectors general reported such a program. In addition, 18 agencies had weaknesses in remediating information security weaknesses in fiscal year 2014. For example, according to the inspector general, components of one agency had inaccurate milestones, did not identify resources to mitigate weaknesses, and had delays in resolving the weaknesses. The Inspector General of that agency also identified 517 milestones that were past due by 12 months.

Without a sound remediation process, agencies have limited assurance that information security weaknesses are being corrected and addressed in a timely manner.

Agencies' Efforts to Implement Incident Response and Reporting Varied

FISMA 2002 required that agency security programs include procedures for detecting, reporting, and responding to security incidents and that agencies report incidents to US-CERT. According to NIST, incident response capabilities are necessary for rapidly detecting an incident, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.⁴⁶

From fiscal year 2013 to fiscal year 2014, agencies' incident response efforts varied. For fiscal year 2014, inspectors general reported that 21 agencies had established an incident response program, which is a slight decrease from fiscal year 2013, in which 22 agencies had established a program. The number of agencies that had routinely reported security incidents to US-CERT within the established time frame also decreased from fiscal year 2013 to fiscal year 2014. Specifically, inspectors general reported that, for fiscal year 2014, 13 agencies had reported incidents to US-CERT within the established time frame, which was a decrease from fiscal year 2013, in which 17 agencies had reported in a timely manner.

Similarly, the number of agencies responding to and resolving incidents also decreased. Specifically, inspectors general reported that, in fiscal year 2014, 15 agencies had responded to and resolved incidents in a

⁴⁶NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61 Revision 2 (Gaithersburg, Md.: August 2012).

timely manner, a decrease from fiscal year 2013, in which 19 agencies had done so. Similar to fiscal year 2013, in fiscal year 2014, according to the inspectors general, 18 agencies had sufficient incident monitoring and detection coverage.

However, inspectors general reported that, in fiscal year 2014, 19 agencies reported incidents to law enforcement, an improvement from fiscal year 2013, in which 18 agencies had done so. Table 4 summarizes agency incident reporting and response practices for fiscal years 2013 and 2014.

Table 4: Agency Incident Reporting and Response Practices as Reported for Fiscal Years 2013 and 2014

Practice	FY 2013	FY 2014	Increase/decrease
Agency reported to US-CERT within established time frames	17	13	Decrease
Agency reported to law enforcement within established time frames	18	19	Increase
Agency responded to and resolved incidents in a timely manner, as specified in organization policy or standards, to minimize further damage	19	15	Decrease
Agency conducted sufficient incident monitoring and detection coverage in accordance with government policies	19	18 [Note A]	Increase

Source: GAO analysis of responses by agency inspectors general to fiscal years 2013 and 2014 FISMA reporting questions. | GAO-15-714

Note A: The Commerce Inspector General reported “not applicable” in this area in fiscal year 2014.

Also, 19 agencies had performed a comprehensive analysis, validation, and documentation of incidents in fiscal year 2014, an improvement of 1 agency over the 18 reported in fiscal year 2013, according to the inspectors general.⁴⁷

Effectively implementing a comprehensive incident detection, reporting, and response program can help agencies better protect their information and information systems from cyber attacks.

⁴⁷In fiscal year 2014, the Commerce Inspector General reported “not applicable” in this area.

Fewer Agencies Had Adequate Contingency Plans

FISMA 2002 required federal agencies to implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. According to NIST, contingency planning is part of overall information system continuity of operations planning, which fits into a much broader security and emergency management effort that includes, among other things, organizational and business process continuity and disaster recovery planning. These plans and procedures are essential steps in ensuring that agencies are adequately prepared to cope with the loss of operational capabilities due to a service disruption such as an act of nature, fire, accident, or sabotage. According to NIST, these plans should cover all key functions, including assessing an agency's IT and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing it and making the necessary adjustments.⁴⁸

Similar to fiscal year 2013, in fiscal year 2014, according to the inspectors general, 17 agencies had established a business continuity and disaster recovery program that was consistent with FISMA 2002 requirements, OMB policy, and applicable NIST guidelines.

The number of agencies that had fully implemented certain key elements of their business continuity and disaster recovery programs decreased, according to the inspectors general. For example, 12 agencies had documented business continuity and disaster recovery plans, a decrease from fiscal year 2013, in which 18 agencies had documented such plans. The inspectors general also reported that several agencies lacked other important elements of a continuity of operations program in fiscal year 2014. For example, 10 agencies had not tested their disaster recovery and business continuity plans, and half of the agencies had not tested system-specific contingency plans. In addition, 7 agencies had not developed or tested contingency plans, trained employees for contingencies, or conducted contingency planning exercises. Further, inspectors general reported that 6 agencies had not established an

⁴⁸NIST, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Revision 1 (Gaithersburg, Md.: May 2010).

alternate processing site for some systems, and 4 agencies had not backed up information in a timely manner.⁴⁹

Weaknesses in continuity of operations could lessen the effectiveness of agencies' efforts to successfully recover their systems in a timely manner after a service disruption occurs.

Agencies Reported Operating Fewer Systems and Relying More on Contractor-Operated Systems

FISMA 2002 required agencies to maintain and update annually an inventory of major information systems (systems) operated by the agency or under its control, which includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.⁵⁰ For fiscal years 2013 and 2014, OMB required agencies to report the number of agency and contractor systems by impact levels.⁵¹

For fiscal year 2014, the 24 agencies reported a total of 9,906 systems, composed of 8,378 agency and 1,528 contractor systems, as shown by impact level in table 5. This represents a slight decrease in the total number of systems from fiscal year 2013, with the number of agency systems decreasing and the number of contractor systems increasing slightly. With respect to impact levels, the total number of low-impact systems decreased while all others, including the number of uncategorized systems, increased. Appendix III lists the number of systems by impact level for each agency, where all agencies reported having moderate-impact systems, five agencies reported not having any high-impact systems, and one agency reported not having any low-impact systems.

⁴⁹In fiscal year 2014, according to OMB, the Commerce Inspector General did not report on the agency's contingency planning program. Therefore, the results of only 23 agencies were included for this area.

⁵⁰FISMA 2002 required federal agencies to maintain an inventory of information systems. Note: The requirement in FISMA 2002 continues in effect at 44 U.S.C. § 3505(c).

⁵¹*Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

Table 5 shows the number of agency and contractor-operated systems by impact level in fiscal years 2013 and 2014.

Table 5: Total Number of Agency and Contractor-Operated Systems Reported for Fiscal Years 2013 and 2014 by Impact Level

Impact level	Agency		Contractor		Total	
	FY 2013	FY 2014	FY 2013	FY 2014	FY 2013	FY 2014
High	835	838	102	120	937	958
Moderate	4,815	4,884	849	882	5,664	5,766
Low	2,768	2,602	332	326	3,100	2,928
Not categorized	52	54	176	200	228	254
Total	8,470	8,378	1,459	1,528	9,929	9,906

Source: GAO analysis of agency fiscal years 2013 and 2014 data. | GAO-15-714

FY—fiscal year

In fiscal years 2013 and 2014, OMB also requested that inspectors general report on agencies' management of contractor systems. Inspectors general reported that 14 agencies had obtained sufficient assurance that security controls of contractor-operated systems and services had been effectively implemented, compared to 13 in fiscal year 2013.

In August 2014, we reported⁵² that five of six agencies we reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls, partly because the agencies had not documented security procedures for effectively overseeing contractor performance. We recommended that five of the six agencies develop procedures for the oversight of contractors. The five agencies generally agreed with the recommendations.

More Agencies Implemented Privacy Requirements

Statutory requirements for the protection of personal privacy by federal agencies are primarily established by the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. In addition, FISMA 2002 addressed the protection of personal information in the context of securing federal agency information and information systems. In addition to these laws, OMB and NIST have issued guidance for assisting

⁵²[GAO-14-612](#).

agencies with implementing federal privacy laws.⁵³ In addition, as part of the annual FISMA reporting process, agencies are required by OMB to report on their progress in implementing federal requirements for protecting the privacy of PII. The requirements include reporting on the implementation of privacy policies and procedures and whether a privacy impact assessment was conducted for systems containing PII.

Agencies reported making progress in implementing federal privacy requirements. For fiscal years 2013 and 2014, according to information from senior agency privacy officials, all 24 agencies reported having written policies and processes for their privacy impact assessment practices. According to OMB, in fiscal year 2014, 95 percent of applicable systems reported by the 24 agencies also had an up-to-date privacy impact assessment.

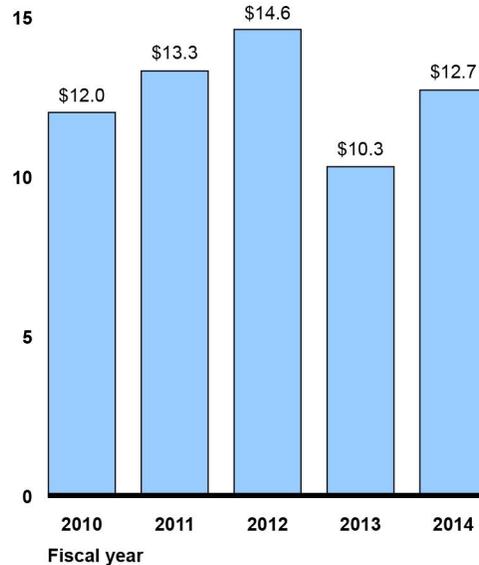
Amount of Spending on Information Security Varied Among Agencies

Each year, OMB requires agencies to report how much their agency spends on information security. From fiscal year 2010 to fiscal year 2014, the 24 agencies reported spending anywhere between 10.3 and 14.6 billion dollars annually on cybersecurity, including 12.7 billion in fiscal year 2014, which is a 23 percent increase from fiscal year 2013 (see fig. 6).

⁵³See, for example, OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003); *Designation of Senior Agency Officials for Privacy*, M-05-08 (Feb. 11, 2005); *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007); and NIST SP 800-53, Revision 4.

Figure 6: Agencies' Reported Cybersecurity Spending

Cybersecurity spending by the 24 major Chief Financial Officers Act agencies (in billions)



Source: GAO analysis of the Office of Management and Budget's fiscal year 2010-2014 annual reports to Congress. | GAO-15-714

For fiscal years 2013 and 2014, agencies reported information security spending in areas that include 1) preventing malicious cyber activity; 2) detecting, analyzing, and mitigating intrusions; and 3) shaping the cybersecurity environment.⁵⁴ The amounts the agencies reported spending in fiscal year 2014 in these three areas are shown in table 6.

⁵⁴ **Preventing malicious cyber activity** pertains to monitoring federal government systems and networks and protecting the data within from both external and internal threats. **Detecting, analyzing, and mitigating intrusions** relates to systems and processes used to detect security incidents, analyze the threat, and attempt to mitigate possible vulnerabilities. **Shaping the cybersecurity environment** aims to improve the efficacy of current and future information security efforts, such as building a strong information security workforce and supporting broader IT security efforts.

Table 6: Reported Fiscal Year 2014 Federal Agencies Cybersecurity Spending by Major Category (amounts in millions)

Agency	Prevent malicious cyber activity	Detect, analyze, and mitigate intrusions	Shaping the cybersecurity environment	Total
Department of Agriculture	\$40	\$46	\$2	\$88
Department of Commerce	56	83	74	213
Department of Education	11	20	1	32
Department of Energy	108	78	71	257
Department of Justice	102	433	44	579
Department of Labor	13	3	1	17
Department of State	55	54	5	114
Department of Transportation	42	44	5	91
Department of Veterans Affairs	13	131	9	153
Department of the Interior	17	30	1	48
Department of the Treasury	122	68	10	200
Department of Defense	2,552	1,225	5,178	8,955
Department of Health & Human Services	54	91	25	170
Department of Homeland Security	473	722	148	1,343
Department of Housing & Urban Development	6	8	0	14
Environmental Protection Agency	1	6	0	7
General Services Administration	27	16	10	53
U.S. Agency for International Development	9	4	3	16
National Science Foundation	3	6	154	163
National Aeronautics & Space Administration	35	48	19	102
Nuclear Regulatory Commission	4	12	3	19
Office of Personnel Management	2	5	0	7
Small Business Administration	1	4	0	5
Social Security Administration	46	11	2	59
Total Cybersecurity Spending	\$3,792	\$3,148	\$5,765	\$12,705

Source: Office of Management and Budget annual report to Congress: *Federal Information Security Management Act*, February 27, 2015. | GAO-15-714

Note: Due to rounding, categories may not sum to the total.

NIST Continues to Provide FISMA-Related Guidance to Agencies

FISMA 2002 established NIST's role of developing information security standards and guidelines for federal agencies such as the *Federal Information Processing Standards* and the special publications in the 800-series for non-national security federal information systems and assigned NIST some specific responsibilities, including the development of:

- Standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.
- Guidelines recommending the types of information and information systems to be included in each category.
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category.

To meet these responsibilities, NIST has continued providing information security guidelines and updates to existing publications. For example, in June of 2014, NIST published *Supplemental Guidance on Ongoing Authorization*, at the request of OMB. This white paper discusses the current set of NIST guidance, and how it supports concepts of ongoing authorizations. Additionally, in September 2014, NIST issued *Special Publication 800-56B, Rev. 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. This publication is intended to provide vendors with information for implementing encryption requirements according to FIPS 140-2.

Table 7 lists the dates for FISMA-related publications that NIST plans to update and issue.

Table 7: NIST FISMA-Related Publications

Issue date	Publication	Description
February 2016 (planned update from revision 1)	NIST SP 800-18, Revision 2, <i>Guide for Developing Security Plans for Federal Information Systems</i>	Provides guidance for federal agencies for developing system security plans for federal information systems
December 2015 (planned update from revision 1)	NIST SP 800-60, Revision 2, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>	Provides guidance to assist agencies in categorizing information and information systems
February 2016 (planned issue)	NIST SP 800-160, <i>Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems</i>	Is intended to provide the engineering-driven actions necessary for developing a more defensible and survivable information technology infrastructure

Source: GAO and NIST's FISMA publication development schedule as of August 2015. | GAO-15-714

Inspectors General Report on Agency Implementation of FISMA

FISMA 2002 required that agencies have an independent evaluation performed each year to evaluate the effectiveness of the agency's information security program and practices. FISMA 2002 also required this evaluation to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) an assessment of compliance with FISMA 2002 requirements, related information security policies, and procedures. For agencies with an inspector general, FISMA 2002 required that these evaluations be performed by the inspector general or an independent external auditor. Lastly, FISMA 2002 required that each year, agencies submit the results of these evaluations to OMB and that OMB summarize the results of the evaluations in its annual report to Congress. According to OMB, the metrics for inspectors general were designed to measure the effectiveness of agencies' information security programs. OMB relies on the responses by inspectors general to gauge the effectiveness of information security program processes.

Agency inspectors general identified weaknesses in agency information security programs and practices in fiscal years 2013 and 2014. They responded to most of the DHS-defined metrics for reporting on agency implementation of FISMA 2002's requirements, and most also issued a detailed audit report discussing the results of their evaluation of agency policies, procedures, and practices.⁵⁵

OMB and DHS Continue Actions, but Opportunities Remain for Improving Annual Reporting of Agency Information Security Programs

FISMA 2002 required that OMB, among other things, oversee and annually report to Congress on agencies' implementation of information security policies, standards, and guidelines. To support its oversight responsibilities, OMB assigned responsibilities to DHS, including overseeing and assisting government efforts to provide adequate, risk-based, cost-effective cybersecurity. OMB and DHS have continued overseeing and assisting agencies with implementing and reporting on cybersecurity, including the following:

⁵⁵OMB noted in its FISMA report to Congress for fiscal year 2014 that one inspector general did not report on cybersecurity programs related to contingency planning and contractor systems. According to OMB, the Commerce Inspector General's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities.

-
- **CyberStat sessions:** According to OMB, these sessions were held with agencies to ensure they are accountable for their cybersecurity posture and to assist them in developing a focused strategy for improving their information security. According to a DHS official, these sessions were held with eight agencies during fiscal year 2013 and four agencies during fiscal year 2014. Beginning in fiscal year 2015, OMB officials stated that that these sessions will be held with agencies with high risk factors, as determined by cybersecurity performance and incident data.
 - **Cybersecurity metrics:** Each year, OMB and DHS provide metrics to federal agencies and their inspectors general for preparing FISMA reports that DHS summarizes for OMB's report to Congress. The metrics listed in the reporting guidance help to form the basis for information on agencies' progress in implementing FISMA requirements and in determining whether agencies have met certain cybersecurity goals set by the current administration.
 - **Proactive scans of publicly-facing agency networks:** In October 2014, OMB instructed DHS and federal agencies to implement a process that allows DHS to conduct regular and proactive vulnerability scans of the publicly-facing segments of the agencies' networks. In addition, DHS is to provide federal agencies with specific results of the scans; offer additional risk and vulnerability assessment services at the request of individual agencies; and report to OMB on the identification and mitigation of risks and vulnerabilities across federal agencies' information systems. According to a DHS official, the department began these scans in February 2015 and has been issuing more than 100 reports per week to federal departments and agencies.

In addition, OMB satisfied its FISMA 2002 requirement to annually report to Congress not later than March 1 of each year on agencies' implementation of the act. OMB transmitted its fiscal year 2014 report on February 27, 2015, to Congress and the Comptroller General. The report highlighted improvements across the federal government such as increases for CAP goals in continuous monitoring, strong authentication, and implementing TIC capabilities. Notwithstanding these improvements, agencies and their inspectors general could further benefit from improved guidance for reporting measures of performance, as described in the next section.

Guidance for Reporting
Agency Evaluations Was Not
always Complete

FISMA 2002 specified that OMB, among its other responsibilities, is to develop policies, principles, standards, and guidelines on information security and report to Congress. Each year, OMB and DHS provide guidance to federal agencies and their inspectors general for preparing their FISMA reports and then summarize the information provided by the agencies and the inspectors general in OMB's annual report to Congress.

For fiscal year 2014 annual FISMA reporting, DHS requested that inspectors general assess their agency's security program in 11 program components (e.g. continuous monitoring, configuration management, security training, among others). For 9 of the 11 program components, the inspector general is first asked to conclude on whether its agency has established a program component that is consistent with FISMA 2002 requirements, OMB policy, and applicable NIST guidelines. Inspectors general are then asked subsequent questions as to whether the program components include certain attributes listed in the reporting instructions. These attributes consist of 5 to 16 additional questions such as whether the agency has documented policies and procedures for that program component or has implemented controls related to that component. Inspectors general are asked to respond to their overall assessment of each program component and the individual attributes using "yes" or "no" responses.

Our review of fiscal year 2014 responses by inspectors general revealed that the reporting guidance was not complete. The lack of appropriate guidance was illustrated by the inconsistent responses to questions supporting their overall evaluation for each of the 11 agency program components. For example, in fiscal year 2014, 19 inspectors general reported that their agency had implemented a continuous monitoring program. Seventeen of the 19 inspectors general reported that their agency's continuous monitoring program included at least 4 of 7 seven attributes or that the attribute was not applicable. However, two of the inspectors general reported their agency had implemented a continuous monitoring program, although those agencies had implemented only 2 of 7 attributes required for the program area.

Other examples we identified illustrate inconsistent inspector general interpretation in reporting. Fifteen of 24 inspectors general reported that their agency had a configuration management program in place and that the program included at least 5 (50 percent) or more of the 10 attributes or that they had not reviewed those attributes. However, 3 other inspectors general reported that their agency had not implemented a configuration management program, even though their program also

included at least 5 (50 percent) or more of the 10 attributes. In addition, another inspector general responded that the program was in place, although only 2 of the 10 configuration management attributes were included in the agency's program.

In our follow-up with the inspectors general, three provided responses illustrating inconsistencies with how they interpreted the annual reporting guidance. Specifically, one pointed out that he based his overall top-level response of "yes" for the program areas on whether more than 50 percent of the attributes were in place at his agency. Another replied that, in addition to OMB and DHS guidance, his agency used an internal threshold of 70 percent for a "yes" answer and that 69 percent and below would result in a "no." The third inspector general responded that he had reviewed five key elements for each component and then evaluated each of the 11 program components by determining whether (1) policies and procedures were in place, (2) controls were designed per policies and procedures, (3) controls were implemented, and (4) controls were operating as intended. These variations in how the guidance was interpreted suggest that additional information on how to incorporate the attributes into the overall conclusion could be valuable in ensuring consistent reporting.

The reporting guidance asks inspectors general for an overall assessment of each program component, but does not define criteria for inspectors general to provide a "yes" or "no" response on whether the program component is implemented. In addition, the guidance does not identify the extent (number or percent of attributes needed for a "yes") to which the attributes should be considered into the overall assessment for each of the components. Therefore, based on our analysis, it appears that some inspectors general reached the same overall assessment, but varied in how those attributes affected their rating. Without complete instructions, differing interpretations of the guidance may therefore result in responses by inspectors general that are not always comparable for presenting a clear government-wide picture of agencies' information security implementation.

Clarifying reporting guidance to inspectors general for the program areas they evaluate would further enhance the quality and consistency of information reported on the government-wide status of federal agencies' implementation of information security policies, procedures, and practices. Without consistent criteria for reporting, inspectors general may be providing Congress and other oversight bodies with uneven

information on the extent to which federal agencies are effectively implementing security requirements.

In the past, we have reported that performance information derived from FISMA reporting provides valuable information on the status and progress of agency efforts to implement effective security management programs, but that shortcomings in the reporting process needed to be addressed. For example, we previously recommended that OMB and DHS provide insight into agencies' security programs by developing additional metrics for key security areas such as those for periodically assessing risk and developing subordinate security plans. We also recommended that metrics for FISMA reporting be developed to allow inspectors general to report on the effectiveness of agencies' information security programs.⁵⁶ OMB and DHS have not yet fully implemented these recommendations.

Conclusions

Federal agencies' information and systems remain at a high risk of unauthorized access, use, disclosure, modification, and disruption. These risks are illustrated by the wide array of cyber threats, an increasing number of cyber incidents, and breaches of PII occurring at federal agencies. Agencies also continue to experience weaknesses with effectively implementing security controls, such as those for access, configuration management, and segregation of duties. OMB and federal agencies have initiated actions intended to enhance information security at federal agencies. Nevertheless, persistent weaknesses at agencies and breaches of PII demonstrate the need for improved security. Until agencies correct longstanding control deficiencies and address the hundreds of recommendations that we and agency inspectors general have made, federal systems will remain at increased and unnecessary risk of attack or compromise.

Federal agencies' implementation of FISMA during fiscal years 2013 and 2014 was mixed. The number of agencies fully implementing components of their security programs increased for some elements, such as developing and documenting policies and procedures, but decreased in others, such as testing controls or providing security training, and varied in implementing incident response and reporting. During fiscal years 2013

⁵⁶GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, [GAO-13-776](#), (Washington, D.C.: September 26, 2013).

and 2014, inspectors general continued to identify weaknesses with the processes agencies used for implementing components of their programs. As a result, agencies are not effectively implementing the risk-based activities necessary for an effective security program required under FISMA 2002 and continued under FISMA 2014.

Although OMB and DHS have increased oversight and assistance to federal agencies in implementing and reporting on information security programs, inconsistencies remain in reporting by inspectors general. Some of these inconsistencies could be alleviated with revised guidance from OMB and DHS. Shortcomings in reporting could result in uneven information being provided to Congress and other oversight entities and limit their ability to compare the extent to which federal agencies are implementing information security programs.

Recommendation for Executive Action

We recommend that the Director of the Office of Management and Budget, in consultation with the Secretary of Homeland Security, the Chief Information Officers Council, and the Council of the Inspectors General on Integrity and Efficiency, enhance reporting guidance to the inspectors general for all rating components of agency security programs, such as configuration management and risk management, so that the ratings will be consistent and comparable.

Agency Comments and Our Evaluation

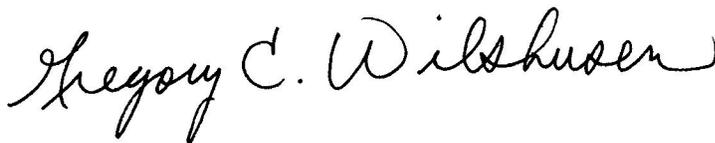
We provided a draft of this report to OMB; DHS; the Departments of Commerce, State, and Treasury; General Services Administration; National Science Foundation; and the Social Security Administration. According to a representative from OMB, the agency generally concurred with our recommendation and provided these comments. During fiscal year 2015, OMB worked with DHS and the Intelligence Community to develop and refine the FY 2016 FISMA metrics. Additionally, OMB continued to work with DHS and the Intelligence Community and has worked with the Chief Information Officers Council and the Information Technology Committee for the Council of the Inspectors General on Integrity and Efficiency to improve the reporting process and enhance FISMA reporting guidance for the inspector general community, respectively.

In written comments (reproduced in appendix IV), SSA's Executive Counselor to the Commissioner stated that the agency takes a proactive approach to identifying and mitigating risk associated with access to their secure network. In e-mail responses, the audit liaison for DHS and

Commerce provided technical comments, which we have incorporated as appropriate. Officials from the Departments of State and Treasury, the General Services Administration, and the National Science Foundation responded that their agency did not have any comments.

We are sending copies of this report to the Director of the Office of Management and Budget, the Secretary of Homeland Security, and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, stylized 'G' and 'W'.

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to evaluate (1) the adequacy and effectiveness of federal agencies' information security policies and procedures and (2) the extent to which federal agencies have implemented the requirements of the *Federal Information Security Management Act (FISMA) of 2002*.

To assess the adequacy and effectiveness of agencies' information security policies and practices, we reviewed and analyzed our, agency, and inspectors general information security-related reports that were issued from October 2013 through May 2015 and covered agencies' fiscal years 2013 and 2014 security efforts. We reviewed and summarized weaknesses identified in these reports using the five major categories of information security general controls identified in our *Federal Information System Controls Audit Manual*: (1) access controls, (2) configuration management controls, (3) segregation of duties, (4) contingency planning, and (5) security management controls.¹ In addition, we reviewed and analyzed financial and performance and accountability reports of the 24 major federal agencies covered by the Chief Financial Officers Act for fiscal years 2013 and 2014.

To evaluate the extent to which the agencies have implemented FISMA's requirements, we reviewed and analyzed the provisions of the 2002 act. We reviewed and analyzed the provisions of the act to identify agency, Office of Management and Budget (OMB), Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST) responsibilities for implementing, overseeing, and providing guidance for agency information security. We did not evaluate agencies' implementation of the *Federal Information Security Modernization Act of 2014* (FISMA 2014), but we compared it to the 2002 act's requirements to identify revised responsibilities for OMB, DHS, and federal agencies. We also reviewed OMB and DHS' annual FISMA reporting guidance, and OMB's annual reports to Congress for fiscal years 2013 and 2014 FISMA implementation. In addition, we analyzed, categorized, and summarized the annual FISMA data submissions for fiscal years 2013 and 2014 by each agency's chief information officer, inspector general, and senior agency official for privacy.²

¹[GAO-09-232G](#).

²The inspector general data submissions and OMB report to Congress did not include information on recommendations that were made to address weaknesses discussed and any actions taken.

To assess the reliability of the agency-submitted data we obtained via CyberScope, we reviewed FISMA reports that agencies provided to corroborate the data.³ In addition, we selected 6 agencies to gain an understanding of the quality of the processes in place to produce annual FISMA reports. To select these agencies, we sorted the 24 major agencies from highest to lowest using the total number of systems each agency had reported in fiscal year 2013; separated them into even categories of large, medium, and small agencies; then selected the last 2 agencies from each category.⁴ These agencies were the Departments of Commerce, State, and the Treasury; the General Services Administration; the National Science Foundation; and the Social Security Administration. We conducted interviews and collected data from the inspectors general and agency officials from the selected agencies to determine the reliability of data submissions. As appropriate, we interviewed officials from OMB, DHS, and NIST. Based on this assessment, we determined that the data were sufficiently reliable for our work.

We conducted this performance audit from December 2014 to September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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.

³CyberScope is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a federal agency's information infrastructure. Agencies are required to use this tool to respond to reporting metrics.

⁴We excluded agencies that had previously been selected for a data reliability assessment in prior years.

Appendix II: Cyber Threats and Exploits

Table 8: Sources of Cybersecurity Threats

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

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center. | GAO-15-714

Table 9: Types of Cyber Exploits

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

Source: GAO data and analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports. | GAO-15-714

Table 10: Cyber Events Characterized by Tactics, Techniques, and Practices

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

Source: NIST. | GAO-15-714

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

Appendix III: Number of Agency and Contractor-Operated Systems by Impact Level

Table 11: Number of Agency and Contractor-Operated Systems in Fiscal Year 2014, by Impact Level

Agency	Agency-operated systems				Contractor-operated systems				Total agency- and contractor-operated systems			
	Impact level			Not categorized	Impact level			Not categorized	Impact level			Not categorized
	H	M	L		H	M	L		H	M	L	
Commerce	19	184	38	0	1	20	6	0	20	204	44	0
DHS	110	354	20	4	14	74	6	1	124	428	26	5
DOD	296	2,231	2,031	18	0	30	65	2	296	2,261	2,096	20
Education	1	18	17	0	1	79	48	0	2	97	65	0
Energy	6	108	14	30	0	167	66	197	6	275	80	227
EPA	1	81	33	0	0	4	2	0	1	85	35	0
GSA	0	37	4	0	6	60	13	0	6	97	17	0
HHS	52	287	89	0	19	119	45	0	71	406	134	0
HUD	0	45	11	0	0	25	1	0	0	70	12	0
Interior	5	98	20	0	3	20	2	0	8	118	22	0
Justice	60	110	29	0	1	12	2	0	61	122	31	0
Labor	0	54	1	0	0	12	0	0	0	66	1	0
NASA	35	228	101	0	0	81	28	0	35	309	129	0
NRC	6	15	0	0	0	1	0	0	6	16	0	0
NSF	0	6	2	0	0	3	0	0	0	9	2	0
OPM	7	18	0	0	6	12	2	0	13	30	2	0
SBA	0	17	1	0	0	8	0	0	0	25	1	0
SSA	0	16	5	0	0	0	0	0	0	16	5	0
State	55	238	14	0	0	3	1	0	55	241	15	0
Transportation	23	211	86	0	11	101	27	0	34	312	113	0
Treasury	39	273	26	0	4	14	1	0	43	287	27	0
USAID	0	22	2	0	2	17	6	0	2	39	8	0
USDA	6	189	56	0	1	13	2	0	7	202	58	0
VA	117	44	2	2	51	7	3	0	168	51	5	2
Total	838	4,884	2,602	54	120	882	326	200	958	5,766	2,928	254

Source: GAO analysis of agency FY 2014 data. | GAO-15-714

Key: H = High; M = Moderate; L = Low.

Note: The Departments of Agriculture (USDA), Commerce, Defense (DOD), Education, Energy, Health and Human Services (HHS), Homeland Security (DHS), Housing and Urban Development (HUD), the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs (VA); the Environmental Protection Agency (EPA); General Services Administration (GSA); National Aeronautics and Space Administration (NASA); National Science Foundation (NSF); Nuclear Regulatory Commission (NRC); Office of Personnel Management (OPM); Small Business Administration (SBA); Social Security Administration (SSA); and the U.S. Agency for International Development (USAID).

Appendix IV: Comments from the Social Security Administration



SOCIAL SECURITY

MEMORANDUM

Date: September 18, 2015

Refer To: SIJ-3

To: Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office

From: Frank Cristaudo *mcrista*
Executive Counselor to the Commissioner

Subject: Government Accountability Office Draft Report, "FEDERAL INFORMATION SECURITY: Agencies Need to Correct Weaknesses and Fully Implement Security Programs" (GAO-15-714) -- INFORMATION

Thank you for the opportunity to review the draft report. We have a strong, proactive approach to the identification and mitigation of risks associated with external and internal access to our secure network. In addition, we have protocols in place that we execute on a continuing basis to identify and mitigate risks and vulnerabilities.

Our efforts were validated in the 2014 Office of Management and Budget Annual Report to Congress on the Federal Information Security Management Act. We scored 96 percent and ranked #1 (shared position) in: automated asset management; detect and block unauthorized software; mobile assets data encryption; vulnerability management; remote access – authentication, connection encryption, timeouts and malware scanning; and email – attachment/web address analysis, digital signature capability, encryption.

We have no further comments. Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Larry Crosland (assistant director), Christopher Businsky, Rosanna Guerrero, Nancy Glover, Angel Ip, Fatima Jahan, Carlo Mozo, and Shaunyce Wallace made key contributions to this report.

Appendix VI: Accessible Data

Data Tables

Data Table for Highlights Figure: Information Security Weaknesses at 24 Federal Agencies in Fiscal Years 2013 and 2014

Number of agencies

Federal information system controls audit manual control areas	FY 2013	FY 2014
Access Control	22	22
Configuration Management	24	22
Segregation of Duties	15	15
Contingency Planning	18	18
Security Management	24	23

Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

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-15-714

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

Category	Number of Incidents	Percentage
Non Cyber	16,879	25%
Scans/Probes/Attempted Access	12,652	19%
Policy Violation	11,588	17%
Equipment	8,798	13%
Malicious Code	7,413	11%
Social Engineering	3,967	6%
Suspicious Network Activity	2,198	3%
Investigation	1,599	2%
Unauthorized Access	1,035	2%

Category	Number of Incidents	Percentage
Improper Usage	760	1%
Phishing	194	0.3%
Denial of Service (DoS)	85	0.1%

Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-714

Data Table for Figure 3: Information Security Weaknesses at the 24 Agencies in Fiscal Years 2013 and 2014

Number of agencies

Federal information system controls audit manual control areas	FY 2013	FY 2014
Access Control	22	22
Configuration Management	24	22
Segregation of Duties	15	15
Contingency Planning	18	18
Security Management	24	23

Source: GAO analysis of agency, inspectors general, and GAO reports issued by May 2015. | GAO-15-714

Data Table for Figure 4: Examples of Agencies' Implementation of Risk Management Program Elements Reported for Fiscal Years 2013 and 2014

Number of agencies

Risk management	FY 2013	FY 2014
Address risk from an organization perspective	12	12
Address risk from a mission and business process perspective	14	16
Address risk from an information system perspective	16	16

Source: GAO analysis of inspectors general *Federal Information Security Management Act* reports for fiscal years 2013 and 2014. | GAO-15-714

Data Table for Figure 5: Agencies' Implementation of Remediation Program Elements Reported for Fiscal Years 2013 and 2014

Number of agencies

Risk management	FY 2013	FY 2014
Tracked Prioritized and Remediate Weaknesses	15	16
Established and Adhered to Milestones Remediation Dates	11	11
Ensured Remediation Plans are Effective	14	16
Resources and ownership provided for correcting weaknesses	14	16

Source: GAO analysis of inspectors general *Federal Information Security Management Act* reports for fiscal years 2013 and 2014. | GAO-15-714

Data Table for Figure 6: Agencies' Reported Cybersecurity Spending

Fiscal year	Cybersecurity spending by the 24 major Chief Financial Officers Act agencies (in billions)
2009	\$6.8
2010	\$12
2011	\$13.3
2012	\$14.6
2013	\$10.3
2014	\$12.7

Source: GAO analysis of the Office of Management and Budget's fiscal year 2010-2014 annual reports to Congress. | GAO-15-714

Agency Comments

Social Security Administration

Accessible Text for Appendix: IV: Comments from the Social Security Administration

SOCIAL SECURITY

MEMORANDUM

Refer to S1J-3

Date: September 18, 2015

To: Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office

From: Frank Cristaudo
Executive Counselor to the Commissioner

Subject: Government Accountability Office Draft Report, "FEDERAL INFORMATION SECURITY: Agencies Need to Correct Weaknesses and Fully Implement Security Programs" (GAO-15-714) -- INFORMATION

Thank you for the opportunity to review the draft report. We have a strong, proactive approach to the identification and mitigation of risks associated with external and internal access to our secure network. In addition, we have protocols in place that we execute on a continuing basis to identify and mitigate risks and vulnerabilities.

Our efforts were validated in the 2014 Office of Management and Budget Annual Report to Congress on the Federal Information Security Management Act. We scored 96 percent and ranked #1 (shared position) in: automated asset management; detect and block unauthorized software;

mobile assets data encryption; vulnerability management; remote access - authentication, connection encryption, timeouts and malware scanning; and email - attachment/web address analysis, digital signature capability, encryption.

We have no further comments. Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#).
Listen to our [Podcasts](#) and read [The Watchblog](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548