United States Government Accountability Office

Report to Congressional Committees

September 2017

FEDERAL INFORMATION SECURITY

Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices

Accessible Version

GAO-17-549

GAO Highlights

Highlights of GAO-17-549, a report to congressional committees

September 2017

FEDERAL INFORMATION SECURITY

Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices

Why GAO Did This Study

GAO first designated federal information security as a governmentwide high-risk area 20 years ago. First enacted in 2002, FISMA required federal agencies to develop, document, and implement information security programs and have independent evaluations of those programs and practices. As amended in 2014, FISMA assigns responsibilities to OMB, DHS, and NIST.

FISMA also includes a provision for GAO to periodically report to Congress on agencies' information security. The objectives of this review are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the extent to which agencies with governmentwide responsibilities have implemented their requirements under FISMA. GAO categorized information security-related weaknesses reported by the 24 CFO Act agencies, their IGs, and OMB according to the control areas defined in the Federal Information System Controls Audit Manual; reviewed prior GAO work; examined OMB, DHS, and NIST documents; and interviewed agency officials.

What GAO Recommends

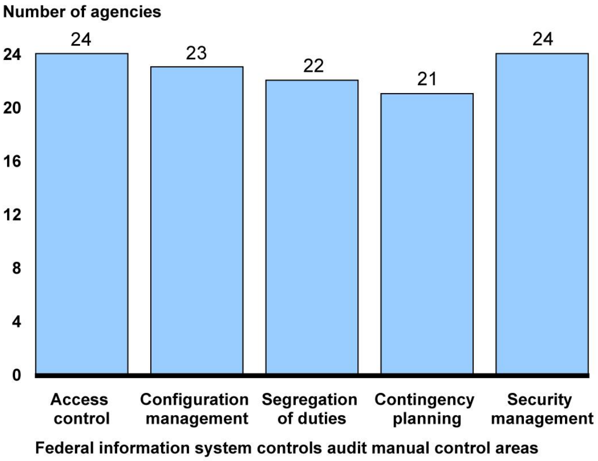
GAO recommends that OMB, in consultation with DHS and others, develop a plan and schedule to evaluate whether the full implementation of the capability maturity model developed by the Council of the Inspectors General on Integrity and Efficiency ensures that consistent and comparable results are achieved across all federal agencies. OMB generally concurred with our recommendation.

View GAO-17-549. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

During fiscal year 2016, federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices. Most of the 24 *Chief Financial Officers Act* (CFO) agencies had weaknesses in five control areas—access controls, configuration management controls, segregation of duties, contingency planning, and agencywide security management (see figure). GAO and inspectors general (IGs) evaluations of agency information security programs, including policies and practices, determined that most agencies did not have effective information security program functions in fiscal year 2016. GAO and IGs have made hundreds of recommendations to address these security control deficiencies, but many have not yet been fully implemented.

The 24 CFO Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 *Chief Financial Officers Act* agencies' information security practices and policies for fiscal year 2016. | GAO-17-549

The Office of Management and Budget (OMB), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and IGs have ongoing and planned initiatives to support implementation of the Federal Information Security Management Act of 2002 as amended by the Federal Information Security Modernization Act of 2014 (FISMA) across the federal government. OMB, in consultation with other relevant entities, has expanded the use of a maturity model developed by the Council of the Inspectors General on Integrity and Efficiency and used to evaluate additional information security performance areas each year. However, OMB and others have not developed a plan and schedule to determine whether using the security capability maturity model will provide useful results that are consistent and comparable. Until an evaluative component is incorporated into the implementation of the maturity model, OMB will not have reasonable assurance that agency information security programs have been consistently evaluated.

Contents

Tables

Figures

Abbreviations

CDM	continuous diagnostics and mitigation
CFO	chief financial officer
DOD	Department of Defense
DHS	Department of Homeland Security
FDA	Food and Drug Administration
FISMA	Federal Information Security Modernization Act of 2014 and Federal Information Security Management Act of 2002
IG	inspector general
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	personal identity verification

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

**441 G St. N.W.
Washington, DC 20548**

September 28, 2017

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

As computer technology has advanced, federal agencies have become dependent on computerized information and electronic data to carry out operations and to process, maintain, and report essential information. Agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, securing these systems and data is vital to the nation’s safety, prosperity, and well-being.

The emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Further, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. The national vulnerability database maintained by the National Institute of Standards and Technology (NIST) has identified 94,901 publicly known cybersecurity vulnerabilities and exposures as of September 19, 2017, with more being added each day.[1]

GAO first designated federal information security as a governmentwide high-risk area 20 years ago in 1997.[2] In 2003,[3] we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015,[4] we further expanded this area to include protecting the privacy of personally identifiable information.[5] We continued to identify federal information security as a government-wide high-risk area in our February 2017 High-Risk update report.[6]

The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program and evaluate it for effectiveness.[7] The act retains many of the requirements for federal agencies' information security programs previously set by the *Federal Information Security Management Act of 2002*[8] and continued responsibilities assigned to the Office of Management and Budget (OMB), NIST, and agency inspectors general. The 2014 law also gave specific oversight responsibilities to the Department of Homeland Security (DHS).

[1] The national vulnerability database is the U.S. government repository of standards based vulnerability management data. The database includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

[2] GAO, *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997).

[3] See 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).

[4] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

[5] Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[6] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb 15, 2017).

[7] The *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.

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

Annually, each federal agency is to have its inspector general (IG) or an independent external auditor perform an independent evaluation to determine the effectiveness of the agency's information security program and practices. The evaluation results are to determine the effectiveness of information security program, policies, procedures, and practices. Agencies are to annually report the results of the evaluation to OMB, and OMB is to summarize those results in annual reports to Congress.

In addition, FISMA included a provision for GAO to periodically report to Congress on agencies' implementation of the act. In this review, our specific objectives were to evaluate (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) the extent to which agencies with governmentwide responsibilities have implemented their requirements under the *Federal Information Security Management Act of 2002* as amended by the *Federal Information Security Modernization Act of 2014* (FISMA).

To address the first objective, we analyzed the provisions of FISMA to identify responsibilities for implementing information security. Using general control categories defined by our *Federal Information System Controls Audit Manual* (FISCAM),[9] we also analyzed, categorized, and summarized control weaknesses identified in our previous information security reports and available reports from the 24 agencies covered by the *Chief Financial Officers Act* (CFO)[10] and agency Offices of Inspector General (OIG) that focused on agencies' information security policies and practices between October 1, 2015 and September 30, 2016.

[9] FISCAM, GAO's audit methodology for performing information system control audits in accordance with generally accepted government auditing standards, defines five categories of general controls: access controls, configuration management, segregation of duties, contingency planning, and security management. These controls include the information security policies and practices that are intended to protect the confidentiality, integrity, and availability of agency information and information systems. See GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

[10] The 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.

In addition, we analyzed available annual agency FISMA reports from 23 civilian CFO Act agencies[11] and OMB's annual report to Congress on agencies' fiscal year 2016 FISMA implementation.[12] We also reviewed OMB's and DHS' annual reporting guidance to the agencies and IGs for fiscal year 2016 FISMA implementation and evaluation.

To determine the reliability of submitted data and obtain clarification about agencies' processes to ensure the accuracy and completeness of data used in their respective FISMA reports, we analyzed documents and conducted interviews with officials from 6 of the 24 CFO Act agencies. For fiscal year 2016, the selected agencies were the Departments of Agriculture, Defense, Housing and Urban Development, and Labor; the National Aeronautics and Space Administration; and the Nuclear Regulatory Commission. For each of our prior three FISMA evaluation reports,[13] we selected six other agencies to reflect a range in the number of systems agencies reported having. The six agencies we reviewed for this current report were selected because they were the remaining agencies not selected in the prior reporting cycles. While not generalizable to all agencies, the information we collected and analyzed about the six selected agencies provided insights into various processes in place to produce FISMA reports. Based on this assessment, we determined that the data were sufficiently reliable for the purposes of our reporting objectives.

To address the second objective we analyzed the FISMA provisions to identify federal responsibilities for overseeing and providing guidance for agency information security. We collected and analyzed documentation related to the coordination among DHS, OMB, and the OIGs to update and refine the FISMA reporting metrics, DHS issuance of binding

[11] According to the Department of Defense (DOD), at the time of our review, DOD had not submitted its FISMA report, nor was it required to issue a financial report for fiscal year 2016.

[12] Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress,* FY 2016 (Washington, D.C.: March 2017).

[13] GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs,* GAO-15-714 (Washington, D.C.: Sept. 29, 2015); GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness,* GAO-13-776 (Washington, D.C.: Sept. 26, 2013); and GAO, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements,* GAO-12-137 (Washington, D.C.: Oct. 3, 2011).

operational directives, newly issued NIST publications, and other governmentwide initiatives to improve federal information security. We also conducted interviews with agency officials at OMB, DHS and NIST to obtain information on their efforts to improve the FISMA reporting process and the cybersecurity posture of the federal government. In addition, we interviewed agency officials to collect information and corroborate documentation of their interaction with OMB and DHS for FISMA activities. For more details on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from October 2016 to September 2017 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.

Background

Threats to IT systems, both intentional and unintentional, are evolving and growing. Unintentional or nonadversarial threat sources include failures in equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters. These threats also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of the control of the organization. Intentional or adversarial threats include individuals, groups, entities, or nations that seek to leverage for illegal purposes the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).

Threats can come from a wide array of sources, including corrupt employees, criminal groups, and terrorists. These threat adversaries vary in terms of their capabilities, their willingness to act, and their motives, which can include seeking monetary gain, or seeking an economic, political, or military advantage.

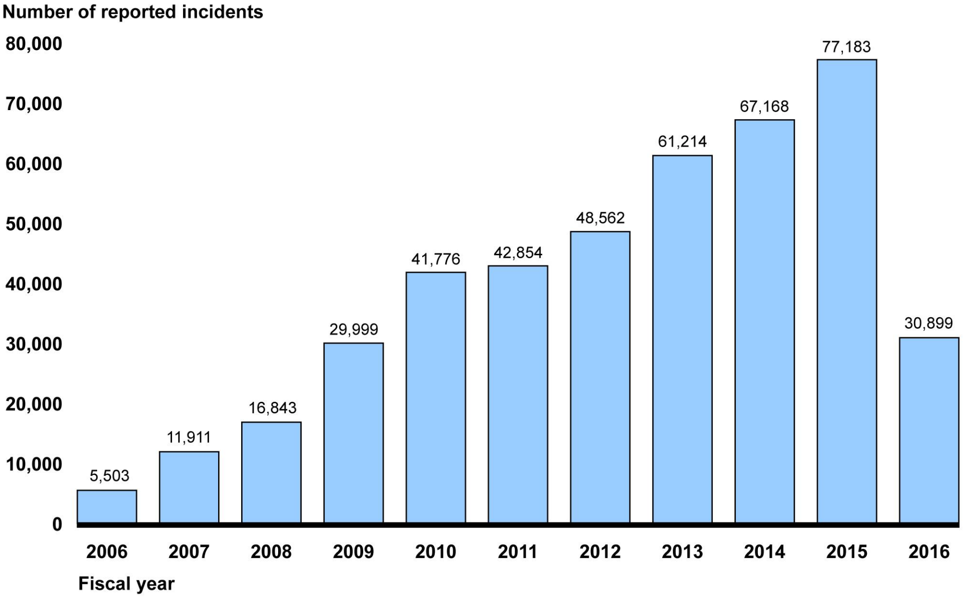
Cyber threat adversaries make use of various techniques, tactics, and practices, or exploits, to adversely affect an organization’s computers, software, or networks, or to intercept or steal valuable or sensitive information. Further, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program. Appendix II contains tables of the sources of cyber-based threats, as well as descriptions of common cyber exploits, and the tactics, techniques, and practices used by cyber adversaries.

Despite a Decrease in Fiscal Year 2016, Federal Agencies Continue to Report Large Numbers of Incidents

Until fiscal year 2016, the number of information security incidents reported by federal agencies to DHS's United States Computer Emergency Readiness Team (US-CERT)[14] had steadily increased each year. From fiscal year 2006 through fiscal year 2015, reported incidents increased from 5,503 to 77,183, an increase of 1,303 percent. However, the number of reported incidents decreased by 60 percent in fiscal year 2016 to 30,899, as shown in figure 1.

[14] US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2006 through 2016



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2016. | GAO-17-549

Note: The decrease in the number of cyber incidents reported in fiscal year 2016 was likely a result of the change in federal incident reporting guidelines. For fiscal year 2016, agencies were no longer required to report non-cyber incidents or incidents categorized as scans, probes, and attempted access. In fiscal year 2015, we reported that that these types of incidents made up 25 percent and 19 percent of the reported types of incidents across the federal government in fiscal year 2014, respectively.

Changes in federal incident reporting guidelines likely contributed to the decrease in reported incidents between fiscal years 2015 and 2016. Updated incident reporting guidelines that became effective in fiscal years 2016 and 2017 no longer required agencies to report noncyber incidents or incidents categorized as scans, probes, and attempted access.[15] In addition, an official from DHS's National Cybersecurity and Communications Integration Center cited the expanded use of the

[15] In 2015, GAO reported that, of the incidents occurring in 2014, noncyber and scans/probes/attempted access incidents accounted for 25 percent and 19 percent of the reported types of incidents across the federal government, respectively. See GAO-15-714 for a breakdown of information security incidents by category for fiscal year 2014.

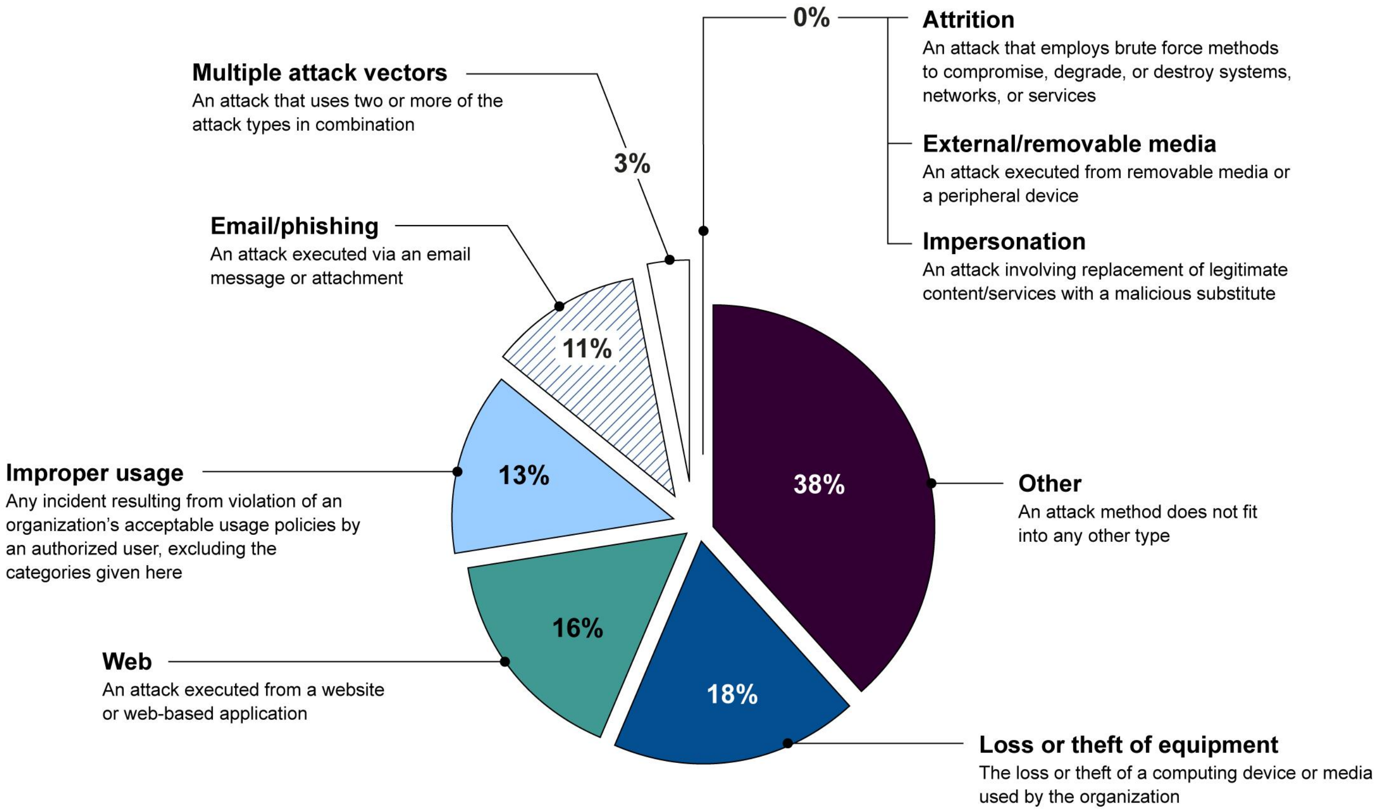
National Cybersecurity Protection System[16] to detect or block potentially malicious network traffic entering networks at federal agencies as another possible reason for fewer reported incidents.

Different types of incidents merit different response strategies; however, if an agency cannot identify the threat vector,[17] it could be difficult for that agency to define more specific handling procedures to respond to the incident. As shown in figure 2, incidents with a threat vector categorized as "other" make up 38 percent of the various incidents reported to US-CERT in fiscal year 2016.

[16] The National Cybersecurity Protection System (NCPS) is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing. See *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C., January 28, 2016) for results of GAO's review of this system.

[17] A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack.

Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2016



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2016. | GAO-17-549

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

- In April 2017, the Commissioner of the Internal Revenue Service (IRS) testified that the IRS had disabled its data retrieval tool in early March after becoming concerned about the misuse of taxpayer data. Specifically, the agency suspected that personally identifiable information obtained outside the agency's tax system was used to access the agency's online federal student aid application in an attempt to secure tax information through the data retrieval tool. In April 2017, the agency began notifying taxpayers who could have been affected by the breach.
- In October 2016, the Department of the Treasury's Office of the Comptroller of the Currency notified us of a major incident it had identified in September 2016. Concurrent with a new policy that

restricted employees’ use of removable media devices to prevent users from downloading information onto the devices without approval and review, the agency began reviewing employee downloads to removable media devices. During the review, it identified a significant change in download patterns for a former employee in the weeks before the employee’s separation from the agency. The former employee had downloaded approximately 28,000 files that may have contained controlled unclassified information onto two encrypted external thumb-drive devices. As of October 2016, the agency had been unable to recover the devices storing the files.

FISMA Establishes Responsibilities for Agencies to Address Federal Cybersecurity

Congress enacted FISMA to improve federal cybersecurity and clarify governmentwide responsibilities. As amended in 2014, the act 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, including:

OMB’s responsibilities

- Develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies except with regard to national security systems.
- Require agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems.
- Ensure that DHS carries out its FISMA responsibilities.
- Coordinate information security policies and procedures with related information resources management policies and procedures.
- Report annually, in consultation with DHS, on the effectiveness of information security policies and practices, including 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.

- Ensure that data breach notification policies and guidelines are periodically updated and require notification to congressional committees and affected individuals.
- Ensure development of guidance for evaluating the effectiveness of an information security program and practices, in consultation with DHS, the Chief Information Officers Council (CIO) Council, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other interested parties, as appropriate.

DHS's responsibilities

- Administer the implementation of agency information security policies and practices for non-national security information systems, in consultation with OMB, including.
    - Assist OMB in fulfilling its FISMA authorities, including the development of policies and oversight of agencies' compliance with FISMA requirements;
    - Develop, issue, and oversee implementation of binding operational directives to agencies, such as those for incident reporting, contents of annual agency reports, and other operational requirements;[18]
    - Monitor agency implementation of information security policies and practices;
    - Convene meetings with senior agency officials to help ensure their effective implementation of information security policies and practices; and
    - Operate the federal information security incident center, deploy technology to continuously diagnose and mitigate threats, compile and analyze data on agency information security, and develop and conduct targeted operational evaluations, including threat and vulnerability assessments of systems.

[18] Binding operational directives are compulsory directions to agencies in order to safeguard federal information and information systems, are in accordance with OMB guidelines, and may be revised or repealed by the OMB director.

NIST's responsibilities

- Establish standards for categorizing information and information systems according to ranges of risk-levels (See *Federal Information Processing Standards* 199 and 200);[19]
- Develop minimum security requirements for information and information systems in each of the risk categories;
- Develop guidelines for detection and handling of information security incidents; and
- Develop guidelines, in conjunction with the Department of Defense, for identifying an information system as a national security system.

Executive branch agencies' responsibilities

- Develop, document, and implement an agencywide information security program that includes the following components:
  - periodic risk assessments, which may include using automated tools consistent with NIST standards and guidelines;
  - policies and procedures that (1) are based on risk assessment, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the lifecycle of each system, and (4) ensure compliance with applicable requirements;
  - plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
  - security awareness training to inform personnel of information security risks and of their responsibilities for 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); such

[19] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004) and National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

testing should include using automated tools consistent with NIST standards and guidelines;

  - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices;
  - procedures for detecting, reporting, and responding to security incidents, which may include using automated tools; and
  - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

- Comply with DHS binding operational directives in addition to OMB policies and procedures and NIST standards.
- Ensure that senior officials carry out assigned responsibilities and that all personnel are held accountable for complying with the agency's information security program.
- Report major security incidents to Congress within 7 days.

In addition, executive branch agencies are to report annually to OMB, certain congressional committees, and the comptroller general of the United States on the adequacy and effectiveness of their information security policies, procedures, and practices, and their compliance with the act. Further, FISMA requires agencies to include descriptions of major incidents in these annual reports. It also requires each agency inspector general, or independent auditor, to annually assess the effectiveness of the information security policies, procedures, and practices of the agency.

The 23 Civilian CFO Act Agencies Reported Information Security Spending

Each year, OMB requires agencies to report how much their agency spends on information security. In fiscal year 2016, each of the 23 civilian agencies covered by the CFO Act reported spending between $3 million and about $1.3 billion on IT security-related activities. Agency reported spending on IT security-related activities ranged between 1 percent and 22 percent of the agencies' IT budget and between 1 percent and 21 percent of their reported IT spending, as seen in table 1.

Table 1: Federal Civilian Agencies' Reported Spending on Information Security for Fiscal Year 2016

Agency[c]	Total IT[a] budget[b] (dollars in millions)	Total IT spending[b] (dollars in millions)	Total IT security spending (dollars in millions)	Percent of IT budget used for IT security	Percent of IT spending used for IT security
Department of Agriculture	$2,789	$3,400	$68	2%	2%
Department of Commerce	2,333	2,300	101	4	4
Department of Education	683	689	81	12	12
Department of Energy	1,496	1,700	334	22	20
Department of Health and Human Services	11,351	13,000	373	3	3
Department of Homeland Security	6,201	6,200	1,284	21	21
Department of Housing and Urban Development	335	342	3	1	1
Department of the Interior	1,099	1,100	73	7	7
Department of Justice	2,732	2,700	207	8	8
Department of Labor	821	714	66	8	9
Department of State	1,632	2,000	127	8	6
Department of Transportation	3,362	3,500	87	3	2
Department of the Treasury	4,503	3,900	396	9	10
Department of Veterans Affairs	4,403	4,400	295	7	7
Environmental Protection Agency	439	425	32	7	7
General Services Administration	602	710	48	8	7
National Science Foundation	102	102	11	11	11
National Aeronautics and Space Administration	1,390	1,400	144	10	10
Nuclear Regulatory Commission	157	153	20	13	13
Office of Personnel Management	127	147	20	16	13
Small Business Administration	102	95	8	8	9
Social Security Administration	1,694	1,500	156	9	10
U.S. Agency for International Development	165	151	25	15	17
TOTAL	**$48,482**	**$50,628**	**$3,958**	**8%**	**8%**

Source: GAO analysis of budget and spending data provided in the President's IT Budget for Fiscal Year 2016, IT Dashboard, and Office of Management and Budget annual *Federal Information Security Modernization Act* report to Congress. | GAO-17-549

[a] Information Technology (IT).

[b] The amounts of information technology and information security spending are self-reported by the agencies.

[c] The Department of Defense was excluded from this analysis because fiscal year 2016 IT security spending data were not available.

Control Weaknesses Indicate Federal Agencies Did Not Adequately or Effectively Implement Information Security Policies and Practices

Weaknesses in security controls such as access controls, configuration management, and security management, indicate that agencies did not adequately or effectively implement information security policies and practices during fiscal year 2016. Further, our work and reviews by inspectors general highlighted 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, many of which have not yet been implemented.

Most of the 24 CFO Act Agencies Exhibited Weaknesses in All Major Categories of Controls

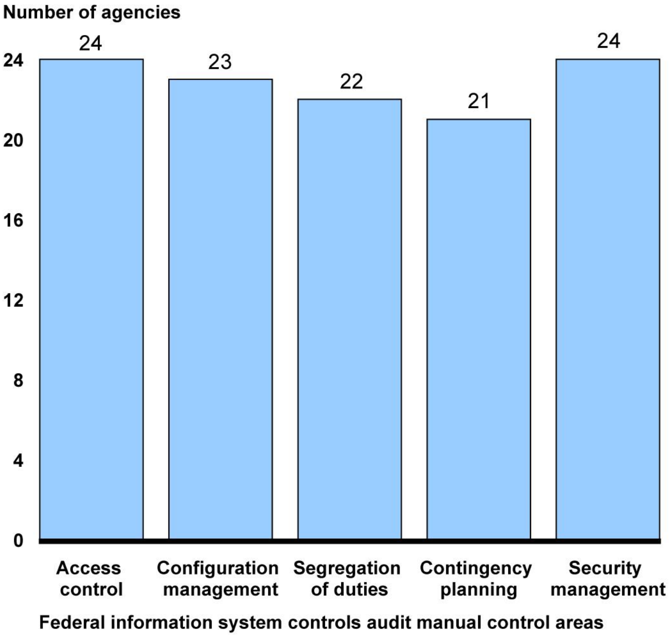
Our reports, agency reports, and inspectors general assessments of information security controls during fiscal year 2016 revealed that most of the 24 agencies covered by the CFO Act had weaknesses in each of the five major categories of information system controls:

- access controls—the policies and practices that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;
- configuration management controls—the policies and practices that are intended to prevent unauthorized changes to information system resources (e.g., software programs and hardware configurations) and to assure that software is current and known vulnerabilities are patched;
- segregation of duties—the policies, practices, and organizational structure that prevent an individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups;
- contingency planning—the policies, plans, and practices that help avoid significant disruptions in computer-dependent operations; and

- agencywide security management—the policies, processes, and practices that provide a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended.

The number of agencies with information security weaknesses in each of the five categories for fiscal year 2016 is shown in figure 3.

Figure 3: The 24 CFO Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 *Chief Financial Officers Act* agencies' information security practices and policies for fiscal year 2016. | GAO-17-549

Note: The 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.

In the following subsections, specific information security weaknesses are discussed that we identified in our analysis of fiscal year 2016 reports reviewed.

All Agencies Had Weaknesses in Access Controls

Agencies design and implement access controls to provide assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals. These controls protect computer resources from unauthorized use, modification, disclosure, and loss by limiting, preventing, or detecting inappropriate access to them. Access controls involve six critical elements:[20]

- boundary protection;
- identification and authentication;
- authorization;
- sensitive system resource protection;
- auditing and monitoring; and
- physical security.

For fiscal year 2016, our analysis identified 516 access control weaknesses at the 24 agencies. The agencies exhibited the most weaknesses in the identification and authentication, authorization, and audit and monitoring critical elements, as shown in table 2.

Table 2: Access Control Weaknesses Reported across the 24 CFO Act Agencies

Critical element	Number of agencies	Number of weaknesses
Boundary protection	20	56
Identification and authentication	24	120
Authorization	24	108
Sensitive system resource protection	13	37
Auditing and monitoring	23	172
Physical security	13	23
Total		**516**

Source: GAO analysis of agency, inspectors general, and GAO reports. | GAO-17-549

[20] Each control category has critical elements, or tasks that are essential for establishing adequate controls within the category.

Boundary Protection

Most of the 24 agencies did not adequately protect information system boundaries. Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices that are connected to a network. In fiscal year 2016, our analysis identified that 20 of the 24 agencies had weaknesses in boundary protection, including not blocking unsecure network traffic and not filtering sensitive data. In addition, our analysis identified other boundary protection weaknesses, such as not authorizing interconnection security agreements for all external systems with connections to internal systems and not requiring the Internet to be accessible only through a trusted Internet connection. Boundary protection-related deficiencies accounted for 56 of the total 516 access control deficiencies identified. Without appropriately controlling connectivity to system resources, agencies risk exploitation of network entry points and access paths by unauthorized users to gain access to sensitive data.

Identification and Authentication

The implementation of effective identification and authentication controls is one of the most widely reported access control weaknesses. Identification and authentication controls allow a computer system to identify and authenticate different users so that activities on the system can be linked to specific individuals.[21] Factors used for authentication include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). Multifactor authentication involves using two or more factors to achieve authentication. In addition, OMB directed agencies to implement the use of personal identity verification (PIV) cards, a form of multifactor authentication, for 85 percent of unprivileged users and 100 percent of privileged users by the end of fiscal year 2016.

Our analysis identified weaknesses in identification and authentication controls at all 24 agencies. Based on the reports analyzed, two agencies

[21] 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.

did not meet the PIV implementation requirement for unprivileged users, five agencies did not meet the requirement for privileged users, and two agencies did not meet the PIV implementation requirement for both unprivileged and privileged users. Identification and authentication related deficiencies accounted for 120 of the 516 total deficiencies found in our analysis. Without implementing adequate logical access controls to appropriately identify and authenticate users, agencies cannot prevent illegitimate users, such as hackers, from accessing systems or restrict legitimate users to only the systems that they need.

Authorization

The implementation of effective authorization controls was a widely reported access control weakness. 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. Agencies should apply the principle of least privilege that requires users to be granted the most restrictive set of privileges needed to perform only the tasks that they are authorized to perform.

Our analysis identified that all 24 agencies had weaknesses in implementing effective authorization controls, which accounted for 108 of the 516 access control weaknesses. For example, three agencies did not periodically review user access to ensure that access was appropriate for the user’s job function. In addition, five agencies had active system accounts for separated employees. Without effective authorization controls, agencies cannot appropriately control user accounts, thereby preventing unauthorized actions by authenticated system users.

Sensitive System Resource Protection

Controls over sensitive system resources are designed to ensure the confidentiality, integrity, and availability of system data, such as passwords and keys during transmission and storage.[22] Cryptography

[22] Three areas related to sensitive system resources are: (1) restricting and monitoring access, (2) implementing adequate media controls over sensitive data, and (3) where appropriate, implementing effective cryptographic controls.

underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information.[23]

Our analysis showed that more than half of the 24 agencies had weaknesses in protecting sensitive system resources. Of the access control weaknesses reported, 37 of the 516 access control weaknesses were related to the protection of sensitive system resources for 13 of the 24 agencies. For example, three agencies did not effectively use encryption to protect sensitive data. If sensitive system resources are not adequately protected, an individual could gain access to capabilities that would allow the individual to bypass security features and, thereby, be able to read, modify, or destroy information or other computer resources.

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.

In fiscal year 2016, our analysis identified 172 auditing and monitoring weaknesses at 23 of 24 agencies. For example, four agencies did not fully implement effective audit and monitoring controls. Two agencies had audit logs to monitor user activity, but did not review them on a consistent basis. In addition, one agency did not consistently identify, notify, or remediate security incidents to ensure incidents were resolved in a timely manner. Without auditing and monitoring system activity, agencies cannot identify indications of inappropriate or unusual activity, thereby hindering agencies' capability to detect, report, and respond to security incidents.

Physical Security

Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. 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

[23] Cryptographic technologies used to control sensitive data include encryption, authentication, digital signature, and key management.

controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security include controlling vehicular and pedestrian traffic. In addition, visitor's access to sensitive areas is to be managed appropriately.

The fewest number of access control weaknesses were identified about physical security. In fiscal year 2016, our analysis identified 23 physical security weaknesses at 13 agencies, including storing switches associated with a data management system in a shared space accessible to people outside of the agency and not retrieving smart identification and PIV cards used to access federal facilities from separated employees. Without adequate physical security controls, agencies cannot restrict physical access to computer resources or protect them from intentional or unintentional loss or impairment.

Overall, our analysis identified access control weaknesses at all 24 agencies. If agencies do not implement security measures to improve access control weaknesses, agencies diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

Agencies Did Not Fully Implement Controls for Configuration Management

Configuration management controls ensure that changes to information system resources are authorized and systems are configured and operated securely and as intended. Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point. It also systematically controls changes to system configurations during the system's life cycle. These controls, which limit and monitor access to powerful programs and sensitive files associated with computer operations, include:

- configuration management policies, plans, and procedures;
- configuration identification;
- configuration change management;
- configuration monitoring;
- patch management; and
- emergency configuration change management.

For fiscal year 2016, our analysis identified 223 configuration management weaknesses at 23 of the 24 CFO Act agencies. As shown in table 3, agencies exhibited the most weaknesses in the critical elements of configuration identification, configuration change management, and patch management.

Table 3: Configuration Management Weaknesses Reported across the 24 CFO Act Agencies

Critical element	Number of agencies	Number of weaknesses
Configuration management policies, plans, and procedures	16	25
Configuration identification	19	56
Configuration change management	20	47
Configuration monitoring	8	13
Patch management	22	82
Emergency configuration change management	0	0
Total		**223**

Source: GAO analysis of agency, inspectors general, and GAO reports. | GAO-17-549

Configuration Management Policies, Plans, and Procedures

Configuration management procedures should cover employee roles and responsibilities, change control and system documentation requirements, establishment of a decision-making structure, and configuration management training. In addition, configuration management should be included in an entity's systems development life cycle methodology, which details procedures that are to be followed when systems and applications are being designed, developed, and modified.

Many of the 24 agencies did not have processes for developing, documenting, and implementing configuration management policies, plans, and procedures. In fiscal year 2016, our analysis identified that 16 of the 24 agencies had weaknesses in developing, documenting, and implementing configuration management procedures. For example, one agency had not developed configuration management standard operating procedures. Another agency had not developed secure baseline configuration guides for its systems. Further, agencies did not implement secure system design, development, and modification procedures. For example, one agency had a web application design flaw that allowed unauthorized users to read and write to the local file system using a vulnerability identified in a software licensing toolkit. Another agency's public-facing website was configured to display error messages that revealed the web server version number and the operating system. Deficiencies related to configuration management procedures accounted for 25 of the total 223 configuration management deficiencies identified during our analysis. Without good configuration management, agencies cannot provide strict control over the implementation of system changes and, thus, minimize corruption to information systems.

Configuration Identification

Configuration identification activities involve identifying, naming, and describing the physical and functional characteristics of a controlled item (for example, specifications, design, Internet protocol (IP) address, code, data element, architectural artifacts, and documents). Agencies should manage a current and comprehensive baseline inventory of hardware, software, and firmware, and it should be routinely validated for accuracy.

Federal agencies had weaknesses reported in maintaining current configuration identification information. In fiscal year 2016, based on our analysis, 19 of the 24 agencies had weaknesses in maintaining configuration identification information. For example, at least three agencies did not have a complete inventory of the hardware, deployed software version, or software license information for the systems used throughout the agencies. Of the 223 configuration management deficiencies that our analysis identified, 56 were related to configuration identification. If agencies do not maintain a current and comprehensive baseline of hardware, software, and firmware, agencies cannot validate configuration information for accuracy, thereby hindering them from controlling changes made to a system.

Configuration Change Management

Configuration change management involves authorizing, testing, approving, tracking, and controlling all configuration changes. A formal change management process allows agencies to create an audit trail to clearly document and track configuration changes.

Based on the reports we reviewed, most of the 24 agencies were not properly managing configuration changes. In fiscal year 2016, 20 of the 24 agencies had weaknesses in configuration change management processes, including failing to consistently implement change management procedures for authorizing, testing, and approving system changes; improperly documenting system change requests; and not tracking approved configuration baseline deviations or changes made to the configuration for verification purposes. Configuration change management accounted for 47 of the 223 configuration management deficiencies identified in our analysis. Without a formal configuration change management process, agencies cannot ensure that systems hardware and related programs operate as intended or that no unauthorized changes are introduced.

Configuration Monitoring

Current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. In addition, security settings for network devices, operating systems, and infrastructure applications need to be monitored periodically to ensure that they have not been altered and that they are set in the most restrictive mode consistent with the information system operational requirements.

Our analysis identified weaknesses in monitoring system configuration. In fiscal year 2016, based on the reports we reviewed, 8 of the 24 agencies had weaknesses in configuration monitoring, including not auditing computer resources on a routine basis to ensure compliance with formally approved baseline standards and failing to review and verify the accuracy of system information. Of the 223 configuration management deficiencies identified in these reports, 13 were related to configuration monitoring. Without monitoring configuration information, agencies cannot adequately protect access paths between information systems. In addition, if agencies do not monitor system security settings, they cannot ensure that the systems have not been altered or that they are consistent with operational requirements.

Patch Management

Software should be scanned and updated frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats. Lastly, software releases should be adequately controlled to prevent the use of noncurrent software.

Based on the reports we analyzed, patch management was the most prevalent configuration management weakness. In fiscal year 2016, our analysis identified that 22 of the 24 agencies had 82 patch management weaknesses. For example, 7 agencies failed to install patches in a timely manner and 6 agencies continued to use software even though it was no longer supported by the vendor.

Emergency Configuration Change Management

Program changes may need to be performed on an emergency basis to keep a system operating. For example, some systems must be continuously available so that the operations they support are not interrupted. In these cases, the risk of missing a deadline or disrupting operations may pose a greater risk than that of temporarily suspending program change controls. However, due to the increased risk that errors or other unauthorized modifications could be introduced, emergency changes should be kept to a minimum. Based on the reports that we analyzed, none of the 24 agencies had weaknesses in appropriately documenting and approving emergency changes to the configuration, based on the reports we reviewed.

Without proper configuration controls, increased risk exists that security features on agency systems could be inadvertently or deliberately omitted or turned off, or that malicious code could be introduced.

More Than Half of the Agencies Did Not Segregate Incompatible Duties

Segregation of duties provides reasonable assurance that incompatible duties are effectively separated and ensures that one individual cannot independently control key aspects of a computer-related operation. Such control would allow that individual to take unauthorized actions or gain unauthorized access to assets or records. Critical elements to achieving adequate segregation include: (1) segregation of incompatible duties and establishment of related policies and (2) controlling employee activity.

In fiscal year 2016, our analysis identified 49 weaknesses in segregation of duties controls at 22 of the 24 agencies. As shown in table 4, agencies exhibited the most weaknesses in the segregation of incompatible duties critical element.

Table 4: Segregation of Duties Weaknesses Reported across the 24 CFO Act Agencies

Critical element	Number of agencies	Number of weaknesses
Segregation of Incompatible duties and establishment of related policies	18	33
Control over employee activity	12	16
Total		**49**

Source: GAO analysis of agency, inspectors general, and GAO reports. | GAO-17-549

Segregation of Incompatible Duties and Establishment of Related Policies

Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing responsibilities this way diminishes the likelihood that errors or wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Agencies had weaknesses in identifying and segregating incompatible duties and establishing related policies. At least seven agencies did not properly segregate personnel responsibilities. For example, one agency combined the roles of the Deputy Chief Information Officer and the Chief Information Security Officer and assigned both to one individual. This meant that one individual performed security control activities at the same time that the person reviewed that activity for compliance with FISMA. Other weaknesses were related to the development of policies and procedures for segregating duties. Deficiencies related to the identification and segregation of duties accounted for 33 of the 49 total segregation-of-duties control deficiencies that we identified in our analysis. If agencies do not effectively segregate incompatible duties and establish related policies, they risk having one individual in control of critical stages of a process, thereby allowing that person to take unauthorized actions or gain unauthorized access to assets or records, possibly without detection.

Control over Employee Activity

Supervision and review of employee activities on a computer system help make certain that users' activities are performed in accordance with prescribed procedures, that mistakes are corrected, and that the computer is used only for authorized purposes.

In fiscal year 2016, our analysis identified 16 weaknesses in control over employee activity at 12 of the 24 agencies. Weaknesses reported include not preventing or detecting segregation of duties conflicts, failing to restrict access to system software, and not reviewing user activity for suspicious or malicious activity. If agencies inadequately control personnel activities, the agencies could allow mistakes to occur and go undetected and facilitate unauthorized use of a computer.

Without adequately segregated duties, agencies increase the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, or computer resources could be damaged or destroyed.

Agencies Had Weaknesses in Contingency Planning

System interruptions can result in the loss of the capability to process, retrieve, and protect electronically maintained information, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. Given the implications of system interruptions, agencies should have procedures for protecting information resources and minimizing the risk of unplanned interruptions. Agencies should also have a plan in place to recover critical operations should interruptions occur. The critical elements of contingency planning include:

- data and operations assessment;
- damage and interruption prevention;
- contingency planning; and
- contingency plan testing.

For fiscal year 2016, as shown in table 5, our analysis identified 106 contingency planning weaknesses. These agencies exhibited the most weaknesses in contingency planning and contingency plan testing.

Table 5: Contingency Planning Weaknesses Reported across the 24 CFO Act Agencies

Critical element	Number of agencies	Number of weaknesses
Data and operations assessment	12	17
Damage and interruption prevention	14	20
Contingency planning	16	34
Contingency plan testing	16	35
Total		**106**

Source: GAO analysis of agency, inspectors general, and GAO reports. | GAO-17-549

Data and Operations Assessment

Agencies should assess the criticality and sensitivity of computerized operations and identify supporting resources. It is important that agencies analyze data and operations to determine which are the most critical and what resources are needed to recover and support them.

In fiscal year 2016, our analysis identified 17 data and operations assessment weaknesses at 12 of the 24 agencies. For example, four agencies' inspectors general reported that their agencies did not consider supply chain threats in their contingency planning. In addition, inspectors general at seven agencies reported that their agency did not incorporate business impact or business process analysis into development of the agencies' contingency planning. If agencies do not identify or prioritize critical data and operations or identify and analyze the resources supporting them, agencies cannot determine which resources merit the greatest protection and what contingency plans need to be made.

Damage and Interruption Prevention

Agencies should take steps to prevent and minimize potential damage and interruption to operations. For examples, agencies can implement capabilities to restore data files, which may be impossible to recreate if lost. In addition, agencies can implement thorough backup procedures and install environmental controls.

In fiscal year 2016, our analysis identified that damage and interruption prevention weaknesses at 14 of the 24 agencies, including failing to retain incremental or full backups and not having an alternate-site redundancy for key mission support information systems. Other weaknesses included not accurately documenting the alternate processing site and backup procedures. Deficiencies related to preventing damage and interruption accounted for 20 of the total 106 contingency planning deficiencies. If agencies do not adequately implement controls to prevent and minimize interruption, agencies risk losing or incorrectly processing data.

Contingency Planning

According to NIST, contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. These plans should be clearly documented, communicated to affected staff, and updated to reflect current operations.

In fiscal year 2016, our analysis identified 34 contingency planning weaknesses at 16 of the 24 agencies. For example, at least three agencies had not updated their contingency plans to reflect the current operating environment. Other contingency planning weaknesses included failure to ensure that business continuity and disaster recovery plans were in place. Without a comprehensive contingency plan in place, agencies can lose the capability to process, retrieve, and protect electronically maintained information, which can affect an agency's ability to accomplish its mission.

Contingency Plan Testing

Testing contingency plans is essential to determining whether they function as intended in an emergency situation. Through this testing, contingency plans can be substantially improved.

Our analysis identified 16 of the 24 agencies had weaknesses in testing their contingency plans. At least five agencies failed to periodically test contingency plans for their systems and one did not provide evidence that it tested contingency plans for all its systems. Of the 106 contingency planning deficiencies that we identified in our analysis, 35 were related to contingency plan testing. If agencies do not test their contingency plans, agencies cannot identify weaknesses in the contingency plans or assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation.

Overall, without effective contingency planning, agencies are unable to ensure that their systems can operate effectively without excessive interruption and can be recovered as quickly and effectively as possible following a service disruption.

Agencies Did Not Effectively Manage Security

An agencywide security program, as required by FISMA, provides a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer related controls through security tests and evaluations, and implementing remedial actions as appropriate. The critical elements for security management include:

- security management program establishment;
- risk assessment and validation;
- security control documentation and implementation;
- security training;
- security program monitoring;
- information security weakness remediation; and
- contractor system review.

For fiscal year 2016, our analysis identified 623 security management weaknesses across the 24 CFO Act agencies. As table 6 shows, agencies exhibited the most weaknesses in the security management program establishment and security program monitoring critical elements.

Table 6: Security Management Weaknesses Reported across the 24 CFO Act Agencies

Critical element	Number of agencies	Number of weaknesses
Security management program establishment	23	161
Risk assessment and validation	20	70
Security control documentation and implementation	22	81
Security training	20	84
Security program monitoring	21	113
Information security weakness remediation	23	58
Contractor system review	20	56
Total		**623**

Source: GAO analysis of agency, inspectors general, and GAO reports. |GAO-17-549

Security Management Program Establishment

An agencywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on an agency's computer resources. Agencies should have a security management structure in place and all policies, plans, and procedures should be kept up-to-date.

In fiscal year 2016, based on the reports we analyzed, 23 agencies had 161 weaknesses in establishing a security management program. These weaknesses included failing to implement an agencywide risk management framework for information security, not ensuring security management policies and procedures are updated, and not designating permanent security management roles and responsibilities. If agencies do not establish a security management program, they may lack a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Risk Assessment and Validation

A comprehensive risk assessment should be the starting point for developing or modifying an agency's security policies and plans. Risk assessments should consider threats and vulnerabilities at the agencywide, system, and application levels, and consider risks to data confidentiality, integrity, and availability. In addition, NIST guidance states that systems should be granted authorization to operate after an authorizing official reviews the system authorization package[24] and determines the risk associated with the system acceptable.

Our analysis identified that 20 of the 24 agencies had weaknesses in assessing and validating risks. For example, at least five agencies allowed systems to continue to operate, even though the system authorizations to operate (ATOs) had expired. Also, risk assessment and validation deficiencies accounted for 70 of the total 623 security management deficiencies. Without a process for periodically assessing and validating risks, agencies cannot ensure that all threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept or mitigate through security controls.

Security Control Documentation and Implementation

Security control policies and procedures should consider risk, address general and application controls, and ensure that users can be held accountable for their actions. They should also be documented and approved by management.

In fiscal year 2016, 22 of the 24 agencies had 81 security control implementation weaknesses based on the reports we analyzed. For example, at least two agencies failed to develop or document security control procedures and at least three agencies did not update security control procedures. In addition, at least one agency did not implement security control procedures. If agencies do not develop, document, update, or implement security control procedures, they cannot ensure that information security is addressed throughout the life cycle of each agency information system.

[24] An authorization to operate is issued when a system's authorizing official reviews the system authorization package and deems the risks associated with the system acceptable. The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls. The authorization package includes a: (1) security plan that provides an overview of security requirements, a description of agreed-upon security controls, and other supporting security-related documents; (2) security assessment report that provides the security control assessment results and recommended corrective actions for control weaknesses; and (3) plan of action and milestones that describes the measures planned to correct weaknesses or deficiencies and to reduce or eliminate known vulnerabilities.

Security Training

An ongoing security awareness program should be implemented that includes first-time awareness training for all new employees, contractors, and users; and periodic refresher training for all employees, contractors, and users. In addition, specialized training for those individuals with significant security responsibilities should be offered. Further, all affected personnel should receive and acknowledge understanding the organization's security policies detailing rules and expected behaviors.

In fiscal year 2016, our analysis identified that 20 of the 24 agencies had weaknesses in implementing a security training program. For example, at least four agencies did not track the status of role-based security training for personnel with significant information security responsibilities. Of the total 623 security management deficiencies identified in our analysis, 84 were related to security awareness training. Without an effective security training program, agencies risk having employees or contractors inadvertently or intentionally compromising security.

Security Program Monitoring

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. Effective monitoring involves agencies performing tests of information security controls to evaluate or determine whether they are appropriately designed and operating effectively. It should also include periodically assessing the appropriateness of security policies and the agency's compliance with them.

In fiscal year 2016, our analysis identified that 21 of the 24 agencies had weaknesses in monitoring their security program, including failing to implement continuous monitoring that requires the validation of compliance with security requirements and not conducting risk management that monitors the selection, implementation, and assessment of security controls. Deficiencies related to security program monitoring accounted for 113 of the total 623 security management deficiencies. Without effectively monitoring agency security programs, agencies cannot ensure that security policies and controls are reducing risk as intended.

Information Security Weakness Remediation

Agencies should have processes for effectively remediating information security weaknesses. When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that the corrective actions are effective. In addition, agencies are to develop plans of actions and milestones (POA&Ms) that describe corrective and remediation actions needed to address identified information security weaknesses. These plans should be based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources.

Twenty-three of the 24 agencies did not have effective processes for remediating information security weaknesses. For example, at least 10 agencies did not remediate identified information security weaknesses in a timely manner. Of those 10 agencies, at least 7 did not use or effectively manage POA&Ms to track, prioritize, and remediate information security weaknesses. Of the 623 security management weaknesses identified in our analysis, we determined that 58 were related to information security weakness remediation. If agencies do not remediate information security weaknesses in a timely manner or use POA&Ms to track the status of identified weaknesses, agencies are exposed to increased risks that nefarious actors will exploit the weaknesses to gain unauthorized access to information resources.

Contractor System Review

Appropriate policies and procedures should be developed, implemented, and monitored to ensure that the activities performed by third parties are documented, agreed to, implemented, and monitored for compliance. In addition, checks should be performed periodically to ensure that the procedures are correctly applied and consistently followed, including the security of relevant contractor systems and outsourced software development.

In fiscal year 2016, our analysis identified 56 weaknesses related to contractor system reviews at 20 of the 24 agencies, including not identifying and maintaining a current system inventory of contractor-operated systems, failing to document or consistently perform procedures for monitoring contractor-operated systems, and failing to perform a formal security assessment of external systems. Without ensuring that external systems are adequately secure, agencies risk having contractors introduce information security risks to their information and systems.

Overall, without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

GAO Has Made Hundreds of Recommendations to Address Cybersecurity Deficiencies That 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 types of risks we found at federal agencies, our recommendations, and the agencies' responses to our recommended actions.

- In August 2016, we reported that the Food and Drug Administration (FDA), an agency of the Department of Health and Human Services, had a significant number of security control weaknesses that jeopardize the confidentiality, integrity, and availability of its information systems and industry and public health data. Specifically, FDA had not fully or consistently implemented access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources. FDA also had weaknesses in other controls, such as those intended to manage the configurations of security features on and control changes to hardware and software; plan for contingencies, including system disruptions and their recovery; and protect media such as tapes, disks, and hard drives to ensure information on them was "sanitized" and could not be retrieved after the hardware was discarded.

  We made 15 recommendations to FDA to fully implement its agencywide information security program. We also recommended that FDA take 166 specific actions to resolve weaknesses in information security controls. The department concurred with our recommendations, has implemented 68 of them, and stated that it is working to address all the recommendations as quickly as possible. The department also stated that FDA has acquired third-party expertise to assist in these efforts to immediately address the recommendations.

- In May 2016, we reported that the National Aeronautical and Space Administration, Nuclear Regulatory Commission, Office of Personnel Management, and the Department of Veteran Affairs had not always effectively implemented access controls over selected high-impact systems. We reported that weaknesses at these agencies also existed in patching known software vulnerabilities and planning for contingencies. An underlying reason for these weaknesses is that the agencies had not fully implemented key elements of their information security programs.

  We made recommendations to each of these agencies to fully implement key elements of their information security programs. The agencies generally concurred with the recommendations, with the exception of the Office of Personnel Management. It disagreed with our recommendation regarding the evaluation of security control assessments to ensure comprehensive testing of technical controls.

- In March 2016, we reported that the Internal Revenue Service had weaknesses in information security controls that limited its effectiveness in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer data. Specifically, the agency had not always (1) implemented controls for identifying and authenticating users, such as applying proper password settings; (2) appropriately restricted access to servers; (3) ensured that sensitive user authentication data were encrypted; (4) audited and monitored systems to ensure compliance with agency policies; and (5) ensured access to restricted areas was appropriate. In addition, unpatched and outdated software exposed it to known vulnerabilities. An underlying reason for these weaknesses is that the Internal Revenue Service had not effectively implemented elements of its information security program.

  We made two recommendations to more effectively implement security-related policies and plans. The Internal Revenue Service agreed with our recommendations and stated that it would review them to ensure that its actions include sustainable fixes that implement appropriate security controls balanced against information technology and human capital resource limitations.

Inspectors General Determined That Federal Agencies Generally Did Not Have Effective Information Security Program Functions

Inspectors general evaluations of agency information security programs, including their respective agencies' policies and practices, determined that most agencies did not have effective information security program functions in fiscal year 2016. The inspectors general evaluated the information security programs for the 24 CFO Act agencies for fiscal year 2016 and determined that only 7 of the 24 agencies had information security programs with any functions considered to be effective.[25] Further, inspectors general from 20 of the 23 civilian agencies cited information security as a "major management challenge" for their respective agency. The inspectors general made numerous recommendations to address these and other issues.

Appendix III provides an overview of the methodology for the inspector general evaluations of their agencies' information security programs and the results of their reviews by agency for fiscal year 2016.

Agencies Acted to Fulfill Their FISMA-defined Roles, but Did Not Sufficiently Plan to Evaluate the Effectiveness of Their Efforts

As required in FISMA, OMB, DHS, NIST, and the agencies' inspectors general have ongoing and planned initiatives to support the act's implementation across the federal government. OMB, among other things, oversaw and reported to Congress on agencies' implementation of information security policies, standards, and guidelines. DHS oversaw and assisted government efforts to provide adequate, risk-based, cost-effective cybersecurity, and NIST developed security standards and guidelines for agencies. Further, agencies' inspectors general conducted annual independent assessments to determine the effectiveness of their respective agencies' information security programs and practices in

[25] NIST defines security control effectiveness as the extent to which security controls are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the information system and are in compliance with established security policies.

accordance with evaluation guidance developed by OMB. However, the oversight agencies do not have plans or a schedule to evaluate the effectiveness of the maturity model developed for inspectors general to evaluate their agencies’ information security programs.

OMB Continued to Provide Guidance for Annual FISMA Reporting and Assistance to Support Agencies' Cybersecurity

FISMA requires that OMB submit a report to Congress no later than March 1 of each year on the effectiveness of agencies' information security policies and practices during the preceding year. This report is to include:

- a summary of incidents described in the agencies' annual reports;
- a description of the threshold for reporting major information security incidents;
- a summary of results the annual IG evaluations of each agency's information security program and practices;
- an assessment of each agency's compliance with NIST information security standards; and
- an assessment of agency compliance with OMB data breach notification policies and procedures.

Although OMB did not meet the deadline of March 1, its annual report to Congress for fiscal year 2016 met the other requirements. Specifically, its report provided an overview of federal cybersecurity, the results of inspectors general evaluations, summaries of agencies' cybersecurity performance, including security incidents reported to US-CERT, and the results of agencies' privacy program performance.[26]

FISMA also required that OMB develop and oversee the implementation of policies, principles, standards, and guidelines on information security. In addition, FISMA required that OMB amend or revise Circular A-130, its policy regarding managing federal information no later than December 18, 2015, a year after FISMA was enacted.

Since we reported in 2015 on FISMA implementation,[27] OMB has developed or revised policies and overseen their implementation as follows:

[26] Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress, FY 2016* (Washington, D.C.: March 2017).

[27] GAO-15-714

- OMB updated and released the revised OMB Circular A-130, *Managing Information as a Strategic Resource*, for comment in October 2015 and released the final version in July 2016, approximately 7 months after the statutory deadline.[28] This circular, last revised in 2000, established general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, information technology resources and supporting infrastructure and services. According to OMB, the latest revised circular reflects changes in law and advances in technology, and represents a shift from viewing security and privacy requirements as compliance exercises to understanding them as crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.
- In October 2015, OMB issued Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan* (CSIP), a guide for federal agencies instructing them to take actions identified as needed through the 2015 30-day Cybersecurity Sprint.[29] The CSIP's key actions included directing agencies to identify their high-value assets and critical system architecture in order to understand the potential impact to those assets and architecture from an adverse cyber incident. The CSIP indicated that progress on the identified actions will be tracked through mechanisms such as comprehensive reviews of agency-specific cybersecurity posture (CyberStats).
- In November 2016, OMB issued Memorandum M-17-05, which included an updated definition of a major information security incident for cyber incident reporting to significantly raise the threshold for an incident to be reported as major.[30] It also updated breach notification policies and requirements for notification to congressional committees and affected individuals. In the updated policy, a breach of personally

[28] Office of Management and Budget, *Managing Information as a Strategic Resource,* Circular No. A-130 (Washington, D.C.: July 2016).

[29] The 30-day Cybersecurity Sprint was a comprehensive review of the federal government's cybersecurity policies, procedures, and practices by the Sprint Team. The goal was to identify and address critical cybersecurity gaps and emerging priorities, and make specific recommendations to address those gaps and priorities.

[30] Per Office of Management and Budget Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, November 4, 2016, OMB redefined a major incident as any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

identifiable information considered to be a major incident, including unauthorized access to 100,000 or more individuals' PII (an increase from the 10,000 threshold in prior guidance), must be reported to Congress within seven days. In addition, OMB's guidance included an incident reporting validation process intended to improve the overall quality of incident data reported.

Further, FISMA directs OMB to oversee agency compliance with requirements to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information or information systems. To fulfill this responsibility, OMB, in coordination with DHS, conducted 24 CyberStat reviews in fiscal year 2016 to help agencies develop action items that address information security risks, identify areas for targeted assistance, and track performance throughout the year.[31] DHS reported that CyberStat reviews were conducted at 16 CFO Act agencies[32] and 7 non-CFO Act agencies during fiscal year 2016 and resulted in 186 cybersecurity-related recommendations that agencies implemented or were in the process of implementing.[33] In addition, OMB conducted a CyberStat review of the continuous diagnostics and mitigation (CDM) program. These reviews revealed cybersecurity issues across the agencies such as high turnover in information technology leadership positions and other workforce challenges, funding mechanisms adversely impacting agencies' cybersecurity posture, immature continuous monitoring programs, and challenges meeting goals for implementing strong authentication methods (e.g., PIV cards).

[31] Per Office of Management and Budget Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, CyberStat reviews are evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing targeted, tactical actions to deliver desired results.

[32] The CFO Act agencies subjected to CyberStat reviews in fiscal year 2016 were the Departments of Agriculture, Commerce, Defense, Education, Energy, the Interior, Health and Human Services, Justice, Labor, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; and the Small Business Administration.

[33] Department of Homeland Security, *2016 CyberStat Reviews: Impact on the State of Cybersecurity* (Washington, D.C.: August 2016).

DHS Issued Cybersecurity-related Directives and Continued to Monitor Cybersecurity Incidents

Under FISMA, DHS, in consultation with OMB, is responsible for carrying out seven activities, including developing information security policies and practices, such as binding operational directives; and overseeing their implementation. In addition, DHS is required to monitor agency implementation of information security policies and practices, meet with senior agency officials to assist with their implementation, and provide operational and technical assistance to agencies.

As required by FISMA, DHS had developed four binding operational directives as of July 2017. These directives instruct agencies to:

- mitigate critical vulnerabilities discovered by DHS's National Cybersecurity & Communications Integration Center (NCCIC) through its scanning of agencies' Internet-accessible systems;[34]
- participate in risk and vulnerability assessments as well as security architecture assessments conducted by DHS on agencies' high-value assets;[35]
- address several urgent vulnerabilities in network infrastructure devices identified in a NCCIC analysis report within 45 days of the directive's issuance; and
- report cyber incidents and comply with annual FISMA reporting requirements.[36]

DHS also provided common security capabilities for agencies in accordance with the FISMA requirement that the department deploy technology, as requested by agencies, to help agencies continuously diagnose and mitigate against cyber threats and vulnerabilities. For example, the National Cybersecurity Protection System (NCPS) (which

[34] Department of Homeland Security, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*, BOD-15-01 (Washington, D.C.: May 21, 2015).

[35] Department of Homeland Security, *Securing High Value Assets*, BOD-16-01 (Washington, D.C.: June 9, 2016).

[36] Department of Homeland Security, *2016 Agency Cybersecurity Reporting Requirements*, BOD-16-03 (Washington, D.C.: Oct. 17, 2016).

includes EINSTEIN)[37] and the CDM program are ongoing DHS initiatives to help secure agency information systems. DHS is accelerating the deployment of CDM and EINSTEIN capabilities to all participating federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats.

- NCPS was developed to be one of the tools to aid federal agencies in mitigating information security threats. The system is intended to provide DHS with the capability to provide four cyber-related services to federal agencies: intrusion detection, intrusion prevention, analytics, and information sharing. In January 2016, we reported that NCPS supported a variety of data analytical tools but had limited intrusion prevention and detection capabilities.[38] In addition, while DHS had developed metrics for measuring the performance of NCPS, the department did not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities.
- CDM is to provide federal departments and agencies with commercial off-the-shelf capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. DHS and the General Services Administration have partnered to implement a blanket purchase agreement available to government entities to acquire and implement CDM tools. In November 2016, DHS awarded a contract for phase 2 of CDM designed to strengthen policies and practices for the authentication of users.

NIST Continues to Provide Information Security Guidance to Agencies

According to FISMA, NIST is to develop information security standards and guidelines, in coordination with OMB and DHS. Specifically, NIST's Computer Security Division is responsible for developing cybersecurity

[37] The National Cybersecurity Protection System (NCPS), operationally known as the EINSTEIN program, is an integrated system-of-systems that is intended to deliver a range of capabilities, including intrusion detection, intrusion prevention, analytics, and information sharing.

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

standards, guidelines, tests, and metrics for the protection of federal information systems.

NIST has developed information security guidelines for federal agencies. Specifically, NIST issued a draft of the revised *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework)[39] in January 2017 in response to feedback and questions received after the original framework's release. The revised framework includes a new section on cybersecurity measurement, an expanded explanation of using the framework for cyber supply chain risk management, and refinements to authentication, authorization, and identity proofing policies within access controls.

In addition, in May 2017, NIST released draft Cybersecurity Framework implementation guidance.[40] The guidance provides federal agencies with approaches to leveraging the framework to address common cybersecurity-related responsibilities. The implementation guidance is intended to assist federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs.[41]

Further, in August 2017, NIST released the initial draft of Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*[42] According to NIST, the update provides a comprehensive set of safeguarding measures for all types of computing platforms and includes security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals. Among the changes in the updated version are the integration of different risk management and cybersecurity approaches including the Cybersecurity Framework and the clarification

[39] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Draft Version 1.1 (Gaithersburg, Md.: Jan. 10, 2017).

[40] National Institute of Standards and Technology, *The Cybersecurity Framework – Implementation Guidance for Federal Agencies,* Draft NISTIR 8170 (Gaithersburg, Md.: May 2017).

[41] On May 11, 2017, the President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which requires each agency to use the Cybersecurity Framework to manage its cybersecurity risk.

[42] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* Special Publication 800-53, Revision 5 (draft) (Gaithersburg, Md.: August 2017).

of the relationship between security and privacy to improve the selection of the appropriate risk mitigating controls.

Inspectors General Evaluated Agency Information Security Programs Using a Maturity Model, but Oversight Agencies Do Not Have a Plan or Schedule for Evaluating the Model's Usefulness

FISMA requires that federal agencies' inspectors general conduct annual independent evaluations to determine the effectiveness of the information security program and practices of their respective agencies based on annually issued OMB guidance. These evaluations are to:

- test the effectiveness of information security policies, procedures, and practices of a subset of agency information systems, and
- assess the effectiveness of an agency's information security policies, procedures, and practices.

We previously reported OMB's FISMA reporting guidance for the inspectors general was not complete and resulted in inconsistent responses to questions in their evaluations.[43] The reporting guidance lacked defined criteria for inspectors general to answer questions about their agencies' information security program components and arrive at an evaluation of the program's effectiveness. We recommended that OMB, DHS, the CIO Council, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) enhance reporting guidance to the inspectors general to achieve more consistent and comparable evaluations.

In fiscal year 2015, CIGIE, in coordination with DHS, OMB, NIST, and other key stakeholders, began developing a security capability maturity model[44] as a methodology to provide an in-depth assessment of agency information security programs. The purpose of the maturity model is to:

- summarize the status of agencies' information security programs;

[43] GAO-15-714.

[44] Capability maturity models contain the essential elements of effective processes for one or more areas of interest and describe an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness. CMMI® for Development, Version 1.3, November 2010.

- provide status about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and
- help ensure consistency across the IG annual FISMA reviews.

The maturity model provides metrics to be used as criteria to evaluate an agency's information security performance areas or domains defined in the annual OMB guidance to the inspectors general for FISMA evaluations.

The inspectors general have implemented the model in phases during their assessments of agency information security programs. In fiscal year 2015, OMB's guidance with reporting metrics directed the inspectors general to use the security capability maturity model to evaluate only one information security function, their agencies' information security continuous monitoring process.[45] In fiscal year 2016, the reporting metrics expanded the use of the security capability maturity model for inspectors general to evaluate their agencies' incident response, as well as information security continuous monitoring programs.

OMB, in consultation with DHS, the CIO Council, and CIGIE, issued fiscal year 2017 FISMA reporting metrics and guidance for the inspectors general that encompasses the full implementation of the security capability maturity model for all security functions.[46] The guidance provides reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs. Further, the guidance instructs the inspectors general to evaluate their agencies' information security programs and assess the effectiveness of the programs using the security capability maturity model. It also states that October 31, 2017, is the deadline for agencies to submit their inspectors general metrics to DHS. Applying the maturity model across all the security functions is to help promote consistent and comparable outcomes from the inspectors general independent annual evaluations.

[45] Information security continuous monitoring (ISCM) provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

[46] Office of Management and Budget, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V 1.0* (Washington, D.C.: April 17, 2017).

Federal guidance and other management practices call for the evaluation of management tools to ensure they are effective. Evaluations of effectiveness should entail assessing whether the tool produces accurate results, can be consistently applied, and is useful in achieving agency objectives. OMB reported that the inspectors general and OMB plan to continue to work together to refine the assessment process and provide methodologies for comparing performance across the government. An official from CIGIE stated that after the full implementation of the security capability maturity model, OMB intends for future guidance to the inspectors general to incorporate measures to address the effectiveness of the model and its use in evaluating agency information security programs. However, the fiscal year 2017 guidance does not include a plan or schedule to determine whether using the security capability maturity model will provide useful results that are consistent and comparable. Until an evaluative component is incorporated into the implementation of the maturity model, OMB will not have reasonable assurance that the inspectors general evaluations of agency information security programs will have consistent and comparable results across all federal agencies as intended.

Conclusions

While federal agencies are working to carry out their FISMA-assigned responsibilities, they continue to experience information security program deficiencies and security control weaknesses in all areas including access, configuration management, and segregation of duties. In addition, the inspectors general evaluations of the information security program and practices at their agencies determined that most agencies did not have effective information security program functions. We are not making new recommendations to address these weaknesses because we and the inspectors general have previously made hundreds of recommendations. Until agencies correct longstanding control deficiencies and address our and agency inspectors general's recommendations, federal IT systems will remain at increased and unnecessary risk of attack or compromise. We continue to monitor the agencies' progress on those recommendations.

Although the inspectors general have continued to implement the security capability maturity model to help ensure more consistency in their program evaluations, OMB, DHS, the CIO Council, and CIGIE have not developed a plan and schedule to evaluate whether the model has achieved useful results that are consistent and comparable as intended.

Further, if OMB, DHS, the CIO Council, and CIGIE, are unable to determine whether using the capability maturity model yields consistent and comparable results, they will not have reasonable assurance that agency information security programs have been consistently evaluated.

Recommendation for Executive Action

We recommend that the Director of the Office of Management and Budget, in consultation with the Secretary of Homeland Security, and the Chief Information Officers Council, evaluate whether the full implementation of the capability maturity model developed by the Council of the Inspectors General on Integrity and Efficiency ensures that consistent and comparable results are achieved across all federal agencies. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB; the Departments of Agriculture, Commerce, Defense, Homeland Security, Housing and Urban Development, and Labor; the National Aeronautics and Space Administration; and the Nuclear Regulatory Commission. Of these agencies, OMB's Program Analyst from the Office of the Federal Chief Information Officer provided comments via e-mail stating that the agency generally concurred with our recommendation. The official added that OMB will continue to work with the Department of Homeland Security, the Chief Information Officers Council, and the Council of the Inspectors General on Integrity and Efficiency to enhance the capability maturity model, and develop a standard methodology that allows for consistent and comparable results across all federal agencies.

In addition, we received written comments from one agency—the Department of Housing and Urban Development—in which it stated that the department had no comment on the draft report. The department added, however, that it is committed to following the established federal laws and guidance and ensuring that its information security program requirements are properly implemented and documented. The department's comments are reprinted in appendix IV.

Further, via e-mail, officials of four agencies—the Department of Agriculture's Senior Advisor for Oversight and Compliance in the Office of the Chief Information Officer; the Department of Labor's representative from the Office of the Assistant Secretary for Policy; the National Aeronautics and Space Administration's audit liaison program manager from the Mission Support Directorate; and the Nuclear Regulatory Commission's executive technical assistant in the Office of the Executive

Director for Operations—responded that their agencies did not have any comments on the draft report.

Finally, in addition to OMB, the Department of Defense; the Department of Homeland Security; and the Department of Commerce's National Institute of Standards and Technology provided technical comments on the draft report, which we incorporated as appropriate.

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 IV.

Gregory C. Wilshusen

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 practices and (2) the extent to which agencies with governmentwide responsibilities have implemented their requirements under the *Federal Information Security Management Act of 2002* as amended by the *Federal Information Security Modernization Act of 2014 (FISMA).*

To assess the adequacy and effectiveness of agencies' information security policies and practices, we analyzed our, agency, and inspectors general (IG) information security-related reports that were issued from October 2015 through January 2017 and covered agencies' fiscal year 2016 security efforts. We analyzed, categorized, 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] We also analyzed, categorized, and summarized the annual FISMA data submissions for fiscal year 2016 by each agency's inspector general. In addition, we analyzed financial reports for fiscal year 2016 for the 23 civilian federal agencies covered by the Chief Financial Officers Act and Office of Management and Budget's (OMB) 2017 annual report to Congress on FISMA implementation.[2] Using cybersecurity spending data provided in OMB's annual FISMA report to Congress and information technology (IT) spending data available on the IT Dashboard, we determined the percentage of IT spending that agencies allotted to IT security in fiscal year 2016.

For the first objective, we also determined the reliability of agency-submitted data at six agencies. To select these agencies for each of our prior three FISMA evaluation reports, we sorted the 24 major agencies from highest to lowest using the total number of systems each agency

[1] GAO-09-232G

[2] We did not receive the DOD Agency Financial Report, which includes the report on top management challenges for the agency. Also, Department of Defense's fiscal year 2016 FISMA report, a classified document, was not issued prior to the fiscal year 2016 OMB report or in time for us to evaluate it for this review.

had reported each year; separated them into even categories of large, medium, and small agencies; then selected the median two agencies from each category.[3] For fiscal year 2016, the Departments of Agriculture, Defense, Housing and Urban Development, and Labor; the National Aeronautics and Space Administration; and the Nuclear Regulatory Commission were the remaining agencies not selected in prior reporting cycles. To assess the reliability of the agency-submitted data, we collected and analyzed documentation of agencies' FISMA reporting processes to determine if they were effective in ensuring the quality of the information reported for FISMA. We also conducted interviews with agency officials to get an understanding of the quality control processes in place to produce the annual FISMA reports. As appropriate, we also interviewed officials from OMB, the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST). While not generalizable to all agencies, the information we collected and analyzed provided insights into various processes in place to produce FISMA reports. Based on this assessment, we determined that the data were sufficiently reliable for the purposes of our objective.

To evaluate the extent to which agencies with governmentwide responsibilities have implemented their FISMA's requirements, we analyzed the provisions of the 2002 and 2014 acts to identify the responsibilities for overseeing and providing guidance for agency information security. We collected documentation of coordination between DHS, OMB, and the IGs to update and refine the FISMA reporting metrics. We also identified DHS-issued binding operational directives, newly issued NIST publications, and other government-wide initiatives to improve federal information security. In addition, we interviewed agency officials to collect information and documentation of their interaction with OMB and DHS for FISMA activities.

We conducted this performance audit from October 2016 to September 2017 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.

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

Appendix II: Cyber Threats and Exploits

Table 7: Sources of Cybersecurity Threats

Source	Description
Nonadversarial/nonmalicious	
Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications.
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies.
Failures in software	Failures in operating systems, networking, and general-purpose and mission-specific applications.
Natural or manmade disaster	Events beyond an entity's control such as fires, floods, tsunamis, tornados, hurricanes, and earthquakes.
Unusual or natural event	Natural events beyond the entity's control that are not considered disasters (e.g., sunspots).
Infrastructure failure or outage	Failure or outage of telecommunications or electrical power.
Unintentional user errors	Failures resulting from erroneous accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities.
Adversarial	
Hacker/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.
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) 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. These individuals engage in purely malicious activities and should not be confused with nonmalicious insider accidents.
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs 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.
Criminal groups and organized crime	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.
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.
Unknown malicious outsiders	Unknown malicious outsiders are threat sources/agents that, due to a lack of information, remain anonymous and are unable to be classified as one of the five types of threat sources/agents listed above.

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-17-549

Table 8: Common Methods of Cyber Exploits

Method of exploit	Descriptions
Watering hole	A method by which threat actors exploit the vulnerabilities of websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cyber-security supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
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 resulting in data loss or corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming instructions (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.
Cross-site request forgery	An exploit that takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory pathname in an application that does not properly neutralize special elements (e.g., '…', '/', '…/') within the pathname.
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	Adversaries manipulate externally controlled format strings in print-style functions to gain access to information and execute unauthorized code or commands.

Open redirect	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site that may contain malware that can compromise the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as "malloc ()".
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., .php) in place of the intended file type (e.g., .jpg).
Inclusion of functionality from un-trusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanisms are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit that combines elements of two or more of the aforementioned techniques.

Source: GAO analysis of unclassified government and nongovernment data. | GAO-17-549

Table 9: 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 malicious 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: National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012). | GAO-17-549

Appendix III: IG Evaluation of Agencies' Information Security Programs

The *Federal Information Security Modernization Act (FISMA) of 2014* requires inspectors general (IG) to independently evaluate the effectiveness of their respective agencies' information security programs and practices. In September 2015, we reported that Office of Management and Budget (OMB) and Department of Homeland Security (DHS) guidance to the inspectors general on conducting and reporting agency evaluations was not always complete and led to inconsistent application.[1] We recommended that DHS and OBM enhance the reporting guidance to facilitate more consistent and comparable inspectors general evaluations.

In fiscal year 2015, the Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE), in coordination with DHS, OMB, the National Institute of Standards and Technology (NIST), and other key stakeholders, began the development of a security capability maturity model to provide an in-depth assessment of agency programs in specific areas. The purpose of the CIGIE maturity model is to:

- summarize the status of agencies' information security programs based on a five-level capability maturity scale;
- provide status about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level; and
- help ensure consistency across the OIGs' annual FISMA reviews.

The five maturity levels used in the IG assessment of agencies' information security programs are defined as follows:

- Level 1 Ad-hoc – Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.

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

- Level 2 Defined – Policies, procedures, and strategy are formalized and documented but not consistently implemented.
- Level 3 Consistently Implemented – Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- Level 4 Managed and Measurable – Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organizations and used to assess them and make necessary changes.
- Level 5 Optimized – Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

OMB's FISMA evaluation guidance identified 11 information security program domains to be addressed in the evaluations: continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.

However, in fiscal year 2015, the maturity model addressed only the information security continuous monitoring domain while the other IG FISMA metric domains were evaluated using sets of independent questions.[2] For fiscal year 2016, the capability maturity model's development continued and expanded to include the incident response domain. Also, CIGIE, OMB and DHS collaborated to align the IG metrics domains with the five function areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): identify, protect, detect, respond, and recover.[3]

Table 10 shows the IGs' FISMA reporting metrics results for the 24 CFO Act agencies by Cybersecurity Framework security function.[4] The IGs'

[2] In fiscal year 2015, the Security Capital Planning domain was incorporated into the Information Security Continuous Monitoring domain, reducing the number of domains to be evaluated to ten.

[3] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, Md.: Feb. 12, 2014).

[4] DOD did not submit metrics to be reported in OMB's fiscal year 2016 report.

evaluations and scoring were based on work performed in fiscal year 2016.

Table 10: Agencies' Inspectors General FISMA Metrics Scores for Fiscal Year 2016

	Cybersecurity functions					
Agency	Identify	Protect	Detect	Respond	Recover	Number of effective functions
Department of Agriculture	L2	L2	L1	L2	L2	0
Department of Commerce	L2	L3	L1	L2	L3	0
Department of Defense	L2	L2	L1	L2	L2	0
Department of Education	L5	L2	L1	L1	L5	2
Department of Energy	L2	L2	L1	L1	L1	0
Department of Health and Human Services	L3	L2	L3	L3	L3	0
Department of Homeland Security	L3	L3	L3	L3	L3	0
Department of Housing and Urban Development	L2	L3	L2	L2	L2	0
Department of the Interior	L2	L2	L1	L1	L2	0
Department of Justice	L3	L3	L3	L3	L4	1
Department of Labor	L2	L2	L2	L1	L5	1
Department of State	L1	L1	L1	L1	L1	0
Department of Transportation	L2	L2	L1	L1	L2	0
Department of the Treasury	L2	L2	L1	L1	L3	0
Department of Veterans Affairs	L2	L3	L2	L3	L3	0
Environmental Protection Agency	L3	L3	L2	L3	L3	0
General Services Administration	L3	L3	L3	L4	L3	1
National Aeronautics and Space Administration	L2	L1	L1	L2	L2	0
National Science Foundation	L3	L3	L4	L4	L5	3

Cybersecurity functions						
Agency	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**	**Number of effective functions**
Nuclear Regulatory Commission	L2	L2	L2	L1	L3	0
Office of Personnel Management	L2	L2	L3	L3	L2	0
Small Business Administration	L2	L2	L2	L2	L5	1
Social Security Administration	L2	L2	L3	L3	L3	0
United States Agency for International Development	L2	L3	L2	L3	L5	1

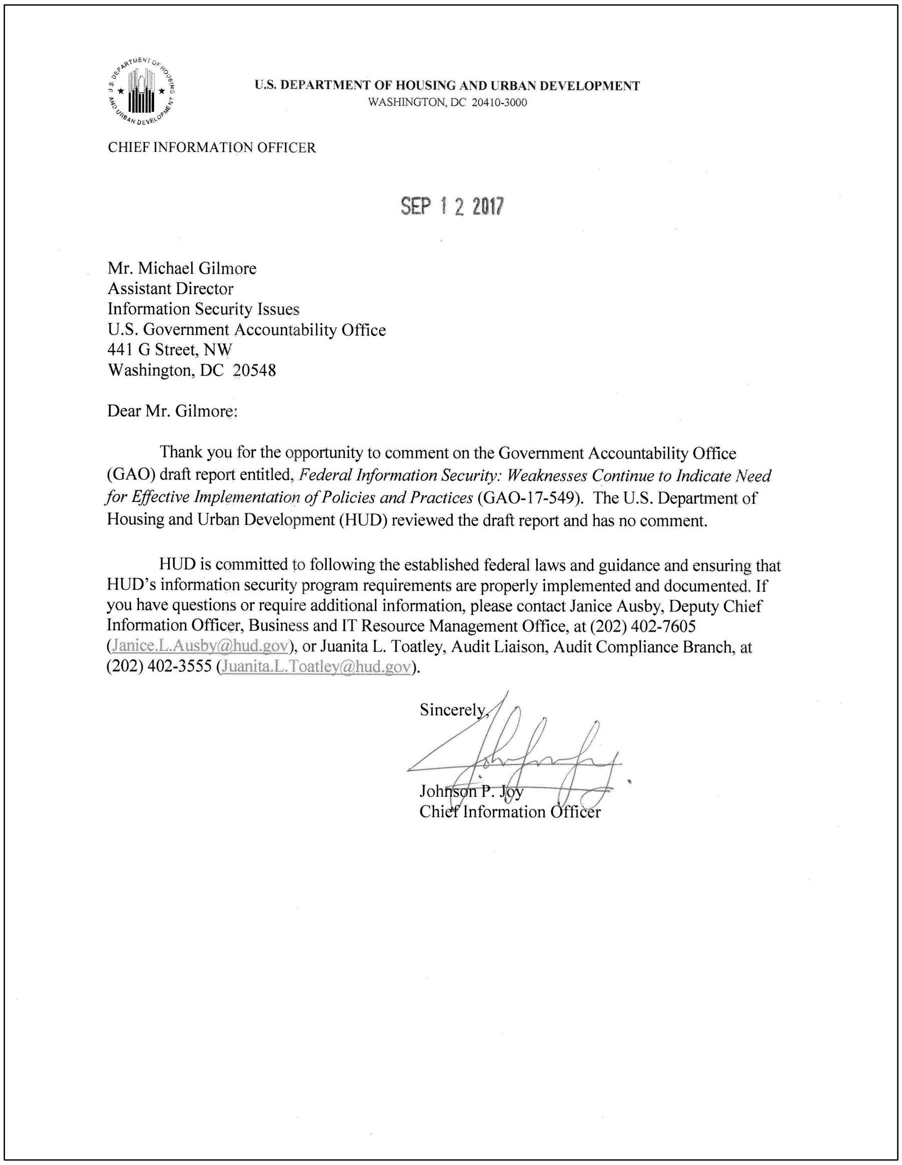
Source: OMB, *FISMA Fiscal Year 2016 Annual Report to Congress* and GAO analysis of agency Inspectors General *Federal Information Security Modernization Act* evaluations. | GAO-17-549

NIST = National Institute of Standards and Technology; Cybersecurity Framework = *Framework for Improving Critical Infrastructure Cybersecurity*; FISMA=*Federal Information Security Modernization Act*.

L1-L5 are Cybersecurity Framework maturity levels achieved by each agency—L1=Level 1, ad-hoc; L2=Level 2, defined; L3=Level 3, consistently implemented; L4=Level 4, managed and measurable; and L5=Level 5, optimized.

Based on the IG evaluations, only 10 information security functions at 7 agencies were determined to be effective (i.e., assessed at, Level 4, managed and measureable, or Level 5, optimized) for fiscal year 2016.

Appendix IV: Comments from the U.S. Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

SEP 12 2017

Mr. Michael Gilmore
Assistant Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Gilmore:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices* (GAO-17-549). The U.S. Department of Housing and Urban Development (HUD) reviewed the draft report and has no comment.

HUD is committed to following the established federal laws and guidance and ensuring that HUD's information security program requirements are properly implemented and documented. If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice.L.Ausby@hud.gov), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

Sincerely,

Johnson P. Joy
Chief Information Officer

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, Michael W. Gilmore and Karl W. Seifert (assistant directors), Kenneth A. Johnson (analyst-in-charge), Kiana Beshir, Christopher Businsky, David Plocher, Di’Mond Spencer, and Priscilla Smith made key contributions to this report.

Appendix VI: Accessible Data

Data Tables

Data Table for Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2006 through 2016

Fiscal Year	Number of Reported Incidents
2006	5503
2007	11911
2008	16843
2009	29999
2010	41776
2011	42854
2012	48562
2013	61214
2014	67168
2015	77183
2016	30899

Data Table for Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2016

Threat Category	Percentage
Other	38%
Loss or Theft of Equipment	18%
Web	16%
Improper Usage	13%
E-mail/Phishing	11%
Multiple Attack Vectors	3%
External/Removable Media	0%
Attrition	0%
Impersonation/Spoofing	0%

Data Table Figure 3: The 24 CFO Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016

Control Category	Number of Weaknesses
Access Control	24
Configuration Management	23
Segregation of Duties	22
Contingency Planning	21
Security Management	24

Agency Comment Letter

Text of Appendix IV: Comments from the U.S. Department of Housing and Urban Development

Mr. Michael Gilmore Assistant Director Information Security Issues

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548 Dear Mr. Gilmore:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled, Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (GAO-17-549). The U.S. Department of Housing and Urban Development (HUD) reviewed the draft report and has no comment.

HUD is committed to following the established federal laws and guidance and ensuring that HUD's information security program requirements are properly implemented and documented. If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice.L.Ausby@HUD.gov) or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at 202-402-3555 (Juanita.L.Toatley@hud.gov) .

Sincerely

Johnson Joy

Chief Information Officer

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, LinkedIn, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov and read The Watchblog.

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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548