



July 2019

FEDERAL INFORMATION SECURITY

Agencies and OMB Need to Strengthen Policies and Practices

Accessible Version

GAO Highlights

Highlights of [GAO-19-545](#), a report to congressional committees

View [GAO-19-545](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

July 2019

FEDERAL INFORMATION SECURITY

Agencies and OMB Need to Strengthen Policies and Practices

Why GAO Did This Study

For 22 years, GAO has designated information security as a government-wide high-risk area. FISMA requires federal agencies to develop, document, and implement information security programs and have independent evaluations of those programs and practices. It also assigns government-wide responsibilities for information security to OMB, DHS, and NIST.

FISMA includes a provision for GAO to periodically report to Congress on agencies' implementation of the act. GAO's objectives in this report were to (1) describe the reported adequacy and effectiveness of selected federal agencies' information security policies and practices and (2) evaluate the extent to which OMB, DHS, and NIST have implemented their government-wide FISMA requirements. GAO categorized information security deficiencies as reported by 16 randomly selected agencies and their IGs according to the elements of an information security program; evaluated IG reports for 24 CFO Act agencies; examined OMB, DHS, and NIST documents; and interviewed agency officials.

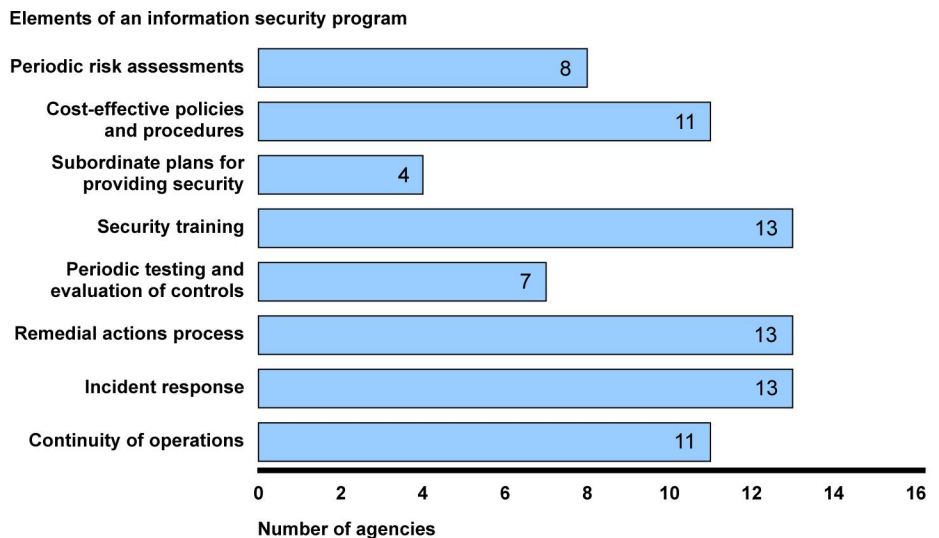
What GAO Recommends

GAO is making three recommendations to OMB to (1) submit its FISMA report to Congress for fiscal year 2018, (2) expand its coordination of CyberStat meetings with agencies, and (3) collaborate with CIGIE to update the inspector general FISMA reporting metrics to include assessing system security plans. OMB generally agreed with GAO's recommendations.

What GAO Found

During fiscal year 2018, many federal agencies were often not adequately or effectively implementing their information security policies and practices. For example, most of the 16 agencies GAO selected for review had deficiencies related to implementing the eight elements of an agency-wide information security program required by the *Federal Information Security Modernization Act of 2014* (FISMA) (see figure). Further, inspectors general (IGs) reported that 18 of the 24 *Chief Financial Officers (CFO) Act of 1990* agencies did not have effective agency-wide information security programs. GAO and IGs have previously made numerous recommendations to agencies to address such deficiencies, but many of these recommendations remain unimplemented.

Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Information Security Program, as Required by the *Federal Information Security Modernization Act of 2014*



Source: GAO analysis of agency, inspector general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-19-545

Data table for Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Information Security Program, as Required by the *Federal Information Security Modernization Act of 2014*

Elements of an information security program	Number of agencies
Periodic risk assessments	8
Cost-effective policies and procedures	11
Subordinate plans for providing security	4
Security training	13
Periodic testing and evaluation of effectiveness	7
Remedial actions process	13

Elements of an information security program	Number of agencies
Incident response	13
Continuity of operations	11

With certain exceptions, the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST) were generally implementing their government-wide FISMA requirements, including issuing guidance and implementing programs that are intended to improve agencies' information security. However, OMB has not submitted its required FISMA report to Congress for fiscal year 2018 and has reduced the number of agencies at which it holds CyberStat meetings from 24 in fiscal year 2016 to three in fiscal year 2018—thereby restricting key activities for overseeing agencies' implementation of information security. Also, OMB, in collaboration with the Council of Inspectors General for Integrity and Efficiency (CIGIE), did not include a metric for system security plans, one of the required information security program elements, in its guidance on FISMA reporting. As a result, oversight of agencies' information security programs was diminished.

Contents

GAO Highlights	2
Why GAO Did This Study	2
What GAO Recommends	2
What GAO Found	2
Letter	1
Background	5
Security Control Deficiencies Reported at Selected Agencies Indicate Ineffective Information Security Policies and Practices	16
OMB, DHS, and NIST Acted to Fulfill Their FISMA-defined Roles, but Shortcomings Exist in Government-wide Efforts Intended to Improve Federal Information Security	45
Conclusions	56
Recommendations for Executive Action	57
Agency Comments and Our Evaluation	57
Appendix I: Objectives, Scope, and Methodology	61
Appendix II: Cybersecurity Framework	65
Appendix III: Comments from the Department of Housing and Urban Development	70
Text of Appendix III: Comments from the Department of Housing and Urban Development	72
Appendix IV: Comments from the Department of Veterans Affairs	74
Text of Appendix IV: Comments from the Department of Veterans Affairs	75
Appendix V: Comments from the Environmental Protection Agency	76
Text of Appendix V: Comments from the Environmental Protection Agency	78

Appendix VI: Comments from the Social Security Administration	79
Text of Appendix VI: Comments from the Social Security Administration	80
Appendix VII: Comments from the U.S. Agency for International Development	81
Text of Appendix VII: Comments from the U.S. Agency for International Development	82
Appendix VIII: GAO Contacts and Staff Acknowledgments	84
GAO Contact	84
Staff Acknowledgments	84

Tables

Data table for Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Information Security Program, as Required by the <i>Federal Information Security Modernization Act of 2014</i>	2
Data table for Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2009 through 2018	7
Data table for Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2018	9
Table 1: Inspector General Evaluation Maturity Levels for Reporting Metrics Associated with the <i>Federal Information Security Modernization Act of 2014</i>	13
Table 2: The 23 Civilian <i>Chief Financial Officers Act of 1990</i> Agencies' Reported Spending on Information Security for Fiscal Year 2018	15
Table 3: Cybersecurity Framework Core Security Functions' Relation to the Inspector General (IG) Reporting Domains	17
Data table for Figure 3: Number of 16 Selected Agencies with Deficiencies in Information Security Policies, Procedures, and Practices, by Core Security Function	18
Data table for Figure 4: Number of 16 Selected Agencies with Deficiencies in Risk Management Activities	20
Data table for Figure 5: Number of 16 Selected Agencies with Deficiencies in the Security Domains Aligned to the Protect Core Security Function	24

Data table for Figure 6: Number of 16 Selected Agencies with Deficiencies in Information Security Continuous Monitoring	29
Data table for Figure 7: Number of 16 Selected Agencies with Deficiencies in Incident Response	32
Data table for Figure 8: Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Agency-wide Information Security Program, as Required by the <i>Federal Information Security Modernization Act of 2014</i>	37
Data table for Figure 9: Inspector General Ratings of 24 <i>Chief Financial Officers Act of 1990</i> Agencies' Information Security Policies, Procedures, and Practices Related to the Cybersecurity Framework Core Security Functions	40
Data table for Figure 10: Number of 24 <i>Chief Financial Officers Act of 1990</i> Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018	42
Table 4: Number of 23 Civilian <i>Chief Financial Officers Act of 1990</i> Agencies Meeting Cross-Agency Priority Goal Targets for 10 Key Milestones	44
Table 5: National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity	65

Figures

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2009 through 2018	7
Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2018	8
Figure 3: Number of 16 Selected Agencies with Deficiencies in Information Security Policies, Procedures, and Practices, by Core Security Function	18
Figure 4: Number of 16 Selected Agencies with Deficiencies in Risk Management Activities	20
Figure 5: Number of 16 Selected Agencies with Deficiencies in the Security Domains Aligned to the Protect Core Security Function	24
Figure 6: Number of 16 Selected Agencies with Deficiencies in Information Security Continuous Monitoring	29

Figure 7: Number of 16 Selected Agencies with Deficiencies in Incident Response	32
Figure 8: Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Agency-wide Information Security Program, as Required by the <i>Federal Information Security Modernization Act of 2014</i>	37
Figure 9: Inspector General Ratings of 24 <i>Chief Financial Officers Act of 1990</i> Agencies' Information Security Policies, Procedures, and Practices Related to the Cybersecurity Framework Core Security Functions	40
Figure 10: Number of 24 <i>Chief Financial Officers Act of 1990</i> Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018	42

Abbreviations

CAP	cross-agency priority
CDM	continuous diagnostics and mitigation program
CFO	chief financial officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
DHS	Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting, and Conformance
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FNR	Federal Network Resilience
HVA	high-value asset
IG	inspector general
IT	information technology
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
US-CERT	United States Computer Emergency Readiness Team

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



July 26, 2019

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

The Honorable Elijah Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

Federal agencies are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

Safeguarding federal computer systems has been a longstanding concern. This year marks the 22nd anniversary of GAO's first designation in 1997 of information security as a government-wide high-risk area.¹ We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003, protecting the privacy of personally identifiable information in 2015, and establishing a comprehensive cybersecurity strategy and performing effective oversight in 2018.² Most recently, we continued to identify federal information

¹GAO, *High-Risk Series: An Overview*, [GAO-HR-97-1](#) (Washington, D.C.: February 1997) and GAO, *High-Risk Series: Information Management and Technology*, [GAO-HR-97-9](#) (Washington, D.C.: February 1997).

²GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 11, 2015) and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: September 6, 2018).

security as a government-wide high-risk area in our March 2019 high-risk update.³

Beginning in fiscal year 2015 through fiscal year 2018, GAO made approximately 1,400 information security-related recommendations. These recommendations identified actions for agencies to take to strengthen their information security programs and technical controls over their computer networks and systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part, because they have not implemented many of these recommendations. As of May 2019, approximately 500 of our prior recommendations had not been implemented.

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 to provide information security for the information and information systems that support the operations and assets for the agency.⁴ FISMA also established government-wide responsibilities that direct the Office of Management and Budget (OMB) to oversee agency information security policies and practices and the Department of Homeland Security (DHS) to administer the implementation of agency information security policies and practices by developing, issuing, and overseeing implementation of binding operational directives. In addition, FISMA 2002 directs the National Institute of Standards and Technology (NIST) to develop standards and guidelines that include minimum information security requirements.

Annually, the inspector general or independent external auditor for each agency is to perform an independent evaluation to determine the effectiveness of the information security policies, procedures, and practices supporting their agency's information security programs. Agencies are to include the results of the evaluations in annual reports that they are required to submit to OMB, certain congressional

³GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: March 6, 2019).

⁴The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

committees, and the Comptroller General. Further, OMB is required to summarize the results in annual reports to Congress.

FISMA also includes a provision for GAO to periodically report to Congress on agencies' implementation of the act. Our specific objectives for this report were to (1) describe the reported adequacy and effectiveness of selected federal agencies' information security policies and practices and (2) evaluate the extent to which OMB, DHS, and NIST have implemented their government-wide FISMA requirements.

To address the first objective, we first reviewed information security-related reports issued by inspectors general and GAO to identify information security deficiencies reported at 16 selected federal agencies.⁵ We analyzed, categorized, and summarized the information security deficiencies identified in these reports according to the (1) five core security functions that make up the *NIST Framework for Improving Critical Infrastructure Cybersecurity* and (2) eight elements of information security programs required by FISMA.⁶

To select the 16 agencies we reviewed, we first ranked the 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) agencies⁷ by the number of information security systems each agency reported operating in fiscal year 2017.⁸ We then separated the agencies into large, medium, and small categories, based on the number of systems they reported, and randomly selected four agencies from each. We also sorted the 73 non-CFO Act agencies identified in OMB's *Fiscal Year 2017 Annual FISMA*

⁵These reports were either issued in fiscal year 2018 or covered fiscal year 2018 (i.e., issued in fiscal year 2019).

⁶National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

⁷The 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) agencies are the Departments of the Agriculture, Commerce, 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 to the 23 civilian agencies, the Department of Defense is part of the 24 CFO Act agencies.

⁸We did not include the Department of Defense in the scope of our selection because the number of systems operated by the department was not publicly reported for fiscal year 2017.

Report to Congress in alphabetical order and randomly selected four non-CFO Act agencies. We chose this sampling strategy to assure a range in agency type (CFO Act and non-CFO Act) and a range in the size (as measured by number of information systems) within our selected agencies. Although we randomly selected agencies and assured we had CFO Act and non-CFO Act agencies, due to the small number of agencies examined, results based on these agencies do not generalize beyond the agencies reviewed.

The 16 selected agencies included 12 CFO Act and four non-CFO Act agencies. The 12 CFO Act agencies were the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency, National Aeronautics and Space Administration, Small Business Administration, and Social Security Administration. The four non-CFO Act agencies were the Federal Communications Commission, Federal Retirement Thrift Investment Board, Merit Systems Protection Board, and Presidio Trust.

In addition, as part of our first objective, we analyzed fiscal year 2018 financial statement audit and FISMA reports issued by the inspectors general for the 24 CFO Act agencies to identify and summarize information security deficiencies described in those reports. Further, for the 23 civilian CFO Act agencies, we analyzed and summarized the FISMA data reported by the agencies' CIOs for fiscal year 2018.⁹

To gain insight into how agencies collect, report, and ensure the accuracy and completeness of their FISMA data, we analyzed documentation describing and supporting the processes at eight of the 16 selected agencies.¹⁰ We also interviewed officials at the eight agencies to obtain additional information on the controls that the agencies used to ensure the quality of FISMA-related data reported to OMB and DHS. The eight agencies selected were the Departments of Education, Justice, Labor, and the Treasury; the Federal Communications Commission; National Aeronautics and Space Administration; Presidio Trust; and the Small Business Administration. Based on our assessment, we determined that

⁹We did not include the Department of Defense in our analysis of fiscal year 2018 FISMA data because the data was classified.

¹⁰These agencies were randomly selected from the list of 16 agencies described above.

the data were sufficiently reliable for the purpose of our reporting objectives.

To address the second objective, we analyzed the FISMA provisions to identify government-wide responsibilities intended to improve the information security of the federal government that have been assigned to OMB, DHS, and NIST. We then evaluated documentation obtained from these agencies and their websites against FISMA requirements. We also interviewed OMB, DHS, and NIST officials to obtain information on any actions they have planned or taken to improve the information security posture of the federal government. For more details on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from December 2018 to July 2019 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

IT systems supporting federal agencies are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising federal systems and networks. Compounding these risks, federal systems and networks are often interconnected with other internal and external systems and networks, including the internet, thereby increasing the number of avenues of attack and expanding their potential attack surface.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Cyber-based threats to information systems can come from sources internal and external to the organization. Internal threats include errors or mistakes, as well as fraudulent or malevolent acts by employees or contractors working within the organization. External threats include the ever-growing number of cyber-based attacks that can come from a

variety of sources such as individuals, groups, and countries that wish to do harm to an organization's systems.

Yet, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety.

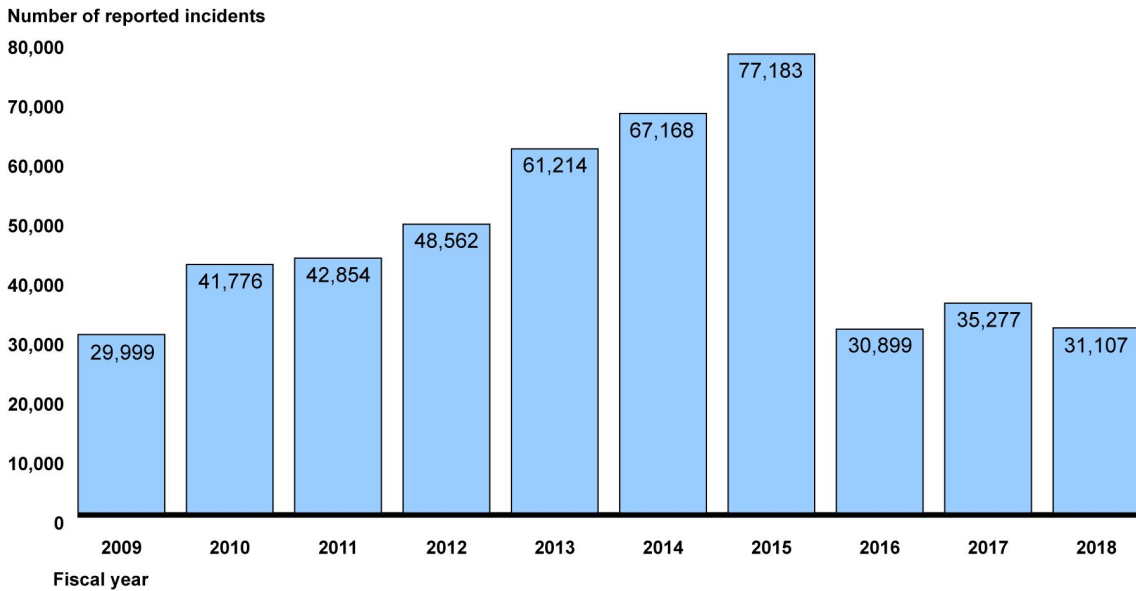
Federal Agencies Continue to Report Large Numbers of Incidents

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) had steadily increased each year.¹¹ From fiscal year 2009 through fiscal year 2015, reported incidents increased from 29,999 to 77,183, an increase of 157 percent. Changes to federal incident reporting guidelines for 2016 contributed to the decrease in reported incidents in fiscal year 2016. Specifically, updated incident reporting guidelines that became effective in fiscal year 2016 no longer required agencies to report non-cyber incidents or incidents categorized as scans, probes, and attempted access.

More recently, agencies reported 35,277 incidents in fiscal year 2017 and 31,107 incidents in fiscal year 2018, as reflected in figure 1.

¹¹US-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 2009 through 2018



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data. | GAO-19-545

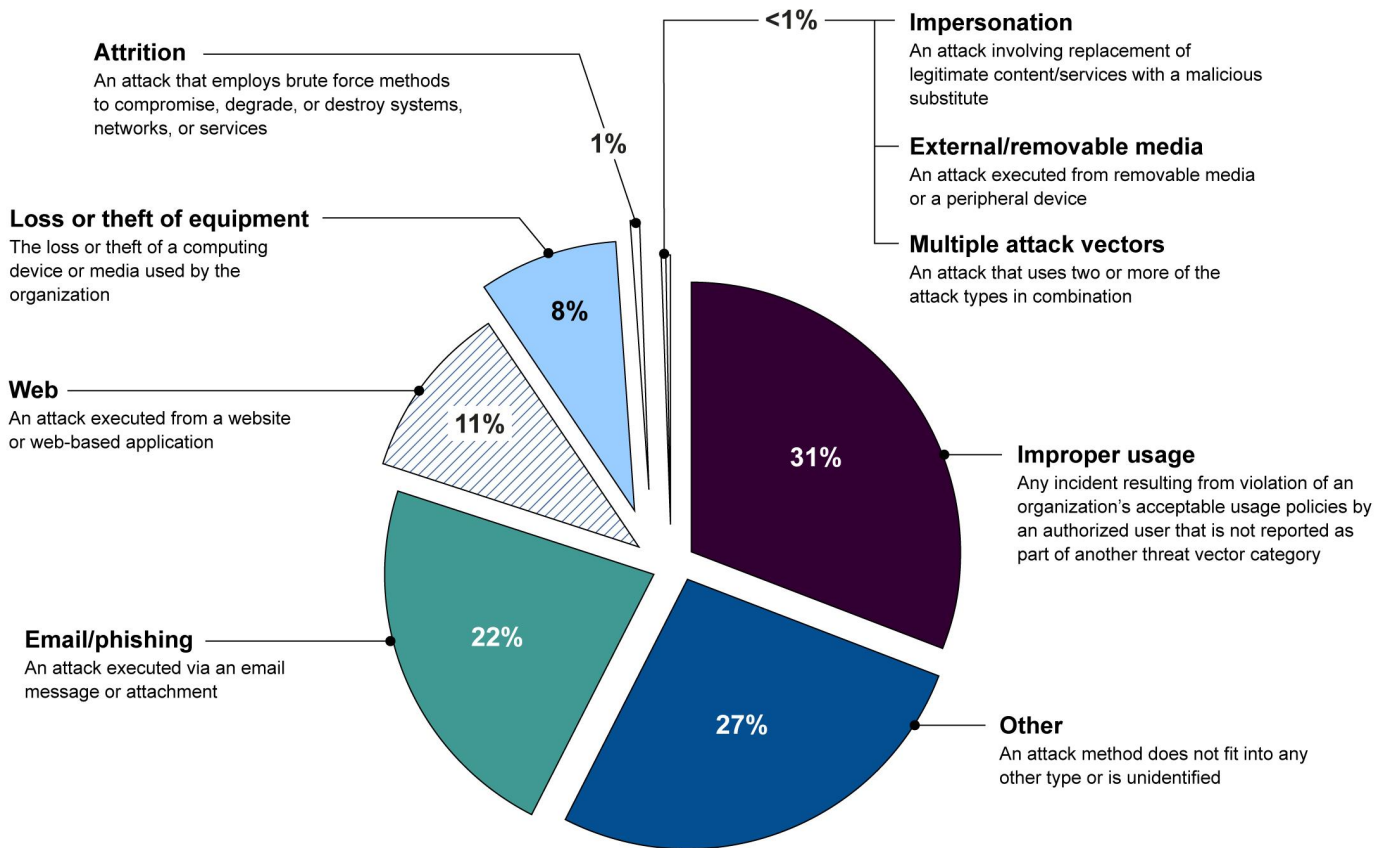
Data table for Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2009 through 2018

Year	Number of reported incidents
2009	29999
2010	41776
2011	42854
2012	48562
2013	61214
2014	67168
2015	77183
2016	30899
2017	35277
2018	31107

According to US-CERT incident report data, the incidents reported in fiscal year 2018 involved several threat vectors.¹² These threat vectors include web-based attacks, phishing attacks, and the loss or theft of computer equipment, among others. Figure 2 provides a breakdown of information security incidents by threat vector in fiscal year 2018.

Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2018

31,107 total information security incidents



Source: United States Computer Emergency Readiness Team incident report data for fiscal year 2018. | GAO-19-545

¹²A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyber attack.

Data table for Figure 2: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2018

Improper Usage	Other	E-mail	Web	Loss or Theft of Equipment	Attrition	Multiple Attack Vectors	Impersonation	External/Removable Media
9674	8285	6930	3332	2552	163	92	47	32

These incidents and others like them can pose a serious challenge to national security, economic well-being, and public health and safety, as shown by two incidents reported in fiscal year 2018:

- In March 2018, the Department of Justice reported that it had indicted nine Iranians for conducting a massive cybersecurity theft campaign on behalf of the Islamic Revolutionary Guard Corps. According to the department, the Iranians allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 U.S. companies, and five federal government agencies, among other entities.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation stated that, since at least March 2016, Russian government actors had targeted U.S. government entities and critical infrastructure sectors, including the energy, nuclear, water, aviation, and critical manufacturing sectors.

FISMA Sets Requirements for Effectively Securing Federal Systems and Information

Congress enacted FISMA 2014 to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and to clarify government-wide responsibilities. The act addresses the increasing sophistication of cybersecurity attacks, promotes the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provides for improved oversight of federal agencies' information security programs.

FISMA requires agencies to develop, document, and implement an agency-wide information security program to secure federal information systems. These information security programs are to provide risk-based protections for the information and information systems that support the operations and assets of the agency. FISMA requires agencies to comply

with OMB policies and procedures, DHS binding operational directives, and NIST federal information standards and guidelines.¹³ In addition, FISMA assigns to agency inspectors general responsibility for annually assessing the effectiveness of the information security policies, procedures, and practices of the agency.¹⁴

FISMA directs OMB to oversee agencies' information security policies and practices. Among other things, FISMA requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems. The law also assigns OMB the responsibility of requiring agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems.

In addition, FISMA 2014 clarified and expanded DHS's responsibilities for government-wide information security. Specifically, the act requires DHS, in consultation with OMB, to administer the implementation of agency information security policies and practices for non-national security information systems by: (1) assisting OMB with carrying out its oversight responsibilities; (2) developing, issuing, and overseeing implementation of binding operational directives; and (3) providing operational and technical assistance.

Further, FISMA 2002 assigned to NIST the responsibility for developing standards and guidelines that include minimum information security requirements.

FISMA also includes reporting requirements. Specifically, OMB is to report annually, in consultation with DHS, on the effectiveness of agency information security policies and practices, including a summary of major agency information security incidents and an assessment of agency compliance with NIST standards. Further, the law requires agencies to report annually to OMB, DHS, certain congressional committees, and the Comptroller General on the adequacy and effectiveness of their

¹³Binding operational directives are compulsory and require agencies to take specific actions to safeguard federal information and information systems from a known threat, vulnerability, or risk.

¹⁴For agencies without an inspector general, the head of the agency shall engage an independent external auditor to perform the evaluation.

information security policies, procedures, and practices, including a description of each major security incident.

Federal Agencies Are Required to Use the Cybersecurity Framework to Manage Risk and to Report on FISMA Implementation

In May 2017, the President signed Executive Order 13800, which sets policy for managing cybersecurity risk as an executive branch enterprise.¹⁵ Specifically, the order outlines actions to be taken by federal agencies and critical infrastructure sectors to improve the nation's cybersecurity posture and capabilities. To this end, the order states that the President will hold executive agency heads accountable for managing agency-wide cybersecurity risk and directs each executive branch agency to use the NIST cybersecurity framework to manage those risks.¹⁶ In addition to requirements set in the executive order, OMB's reporting metrics that were developed to facilitate agencies' compliance with FISMA's reporting requirement are aligned to the core functions outlined in the cybersecurity framework. Consequently, agencies are required to report on the effectiveness of their information security policies and practices according to the cybersecurity framework's core functions.

NIST Framework's Five Core Functions Are Aimed at Managing Cybersecurity Risk

The NIST cybersecurity framework is based on five core security functions:

- Identify: Develop an understanding of the organization's ability to manage cybersecurity risk to systems, people, assets, data, and capabilities.

¹⁵The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017), 82 Fed. Reg. 22391 (May 16, 2017).

¹⁶The framework was developed in response to an executive order issued by the prior administration, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013). It was originally intended for use in protection of critical infrastructure. NIST initially issued guidance in February 2014 and has since revised the framework.

- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.¹⁷
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

According to NIST, these five functions should be performed concurrently and continuously to address cybersecurity risk. In addition, when considered together, they provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk. Within the five functions, NIST identifies 23 categories and 108 subcategories of activities and controls for achieving the intent of each function.¹⁸ Appendix II provides a description of the cybersecurity framework categories and subcategories of activities and controls.

Inspectors General Are to Measure the Effectiveness of Agencies' Information Security Programs Using the Cybersecurity Framework Core Functions

The Council of Inspectors General for Integrity and Efficiency (CIGIE), in collaboration with OMB, DHS, and other stakeholders, developed a capability maturity model for agency inspectors general to assess and report on the effectiveness of their agencies' information security programs. As described in table 1, the model identifies five maturity levels with each succeeding level representing a more advanced level of implementation.

¹⁷Cybersecurity events are cybersecurity changes that may have an impact on the organizational operations (including mission, capabilities, or reputation).

¹⁸For example, "risk assessment" is one of five categories that comprise the "identify" function. The risk assessment category is divided into six subcategories that involve activities such as: identifying and documenting internal and external threats; identifying potential business impacts and likelihoods; and determining risk based on threats, vulnerabilities, likelihoods, and impacts. Each subcategory activity cross-references information system controls from various information security publications.

Table 1: Inspector General Evaluation Maturity Levels for Reporting Metrics Associated with the *Federal Information Security Modernization Act of 2014*

Maturity level	Description
Level 1: Ad hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies 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 strategies are collected across the organization and used to assess those policies, procedures, and strategies, and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: GAO analysis of FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.0.1 May 24, 2018. | GAO-19-545

Using the five-level maturity model described above, the inspectors general are to assign a maturity-level rating for each of the five core security functions based on an assessment of their agencies' implementation of the activities and controls associated with each function using metrics that CIGIE developed in collaboration with OMB.¹⁹ The inspectors general then consider the maturity level ratings of the core security functions to evaluate the overall effectiveness of their agency's information security program.

OMB instructs inspectors general to rate their agency's information security program as effective or not effective by applying a rule of simple majority. Specifically, if three or more of the five core security functions are rated effective, the overall information security program is considered to be effective.²⁰ According to this maturity model, Level 4 (managed and measurable) is the lowest level to represent an effective level of

¹⁹Inspector general FISMA metrics and reporting instructions were developed as a collaborative effort amongst OMB, DHS, and CIGIE. The metrics provide reporting requirements across key areas to be addressed in the independent assessment of agencies information security programs. See *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.01 (May 24, 2018).

²⁰Inspectors general have the discretion to determine the overall agency information security program rating and the rating for each of the cybersecurity framework functions at the level of their choosing.

security.²¹ Therefore, if an inspector general rates three or more of the agency's core security functions at Level 4 or Level 5, then the inspector general can consider that agency to have an effective information security program. However, the inspector general has the discretion to have a different conclusion on program effectiveness if he or she deems it appropriate to do so.

CIOs Are Required to Assess Agencies' Progress in Implementing Capabilities Related to the Administration's Cybersecurity-related Cross-Agency Priority Goal

Similar to the inspector general FISMA reporting metrics, OMB and DHS worked with interagency partners to develop the CIO FISMA metrics, which are intended to be used by the agencies, OMB, and DHS to track agencies' progress in implementing cybersecurity capabilities. The CIO FISMA reporting metrics are organized around the five core security functions outlined in NIST's cybersecurity framework.

In addition, certain CIO FISMA reporting metrics represent key milestones of the administration's IT Modernization Cross-Agency Priority (CAP) goal, which includes a cybersecurity initiative.²² As a result, the CIO reporting metrics allow agency CIOs, OMB and DHS to monitor progress toward meeting key milestones and targets for the CAP goal.

The cybersecurity initiative within the IT Modernization CAP goal is designed to reduce cybersecurity risks to the federal government's information systems by mitigating the impact of risks to federal data, systems, and networks. The initiative consists of three strategies that contain 10 milestones that relate to key areas within the CIO FISMA metrics—information security continuous monitoring; identity, credential, and access management; and advanced network and data protections. In

²¹NIST defines security control effectiveness as the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system and are in compliance with established security policies.

²²The President's Management Agenda is intended to lay out a long-term vision for modernizing the federal government in key areas that will improve the ability of agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people. The Cross-Agency Priority goals described within the President's Management Agenda are 4-year outcome-oriented goals that measure federal progress toward implementing the agenda.

addition, each of the 10 milestones has an expected level of performance, or target, for implementation, as described later in this report.

Reported Information Security Spending Varies Among the 23 Civilian CFO Act Agencies

Each year, OMB requires agencies to report how much they spend on information security. In fiscal year 2018, the 23 civilian agencies covered by the CFO Act reported spending between \$9 million and almost \$1.9 billion on cybersecurity- or IT security-related activities. For these 23 agencies, their total reported security spending accounted for about 14 percent of their IT spending, with percentages for individual agencies ranging from 5 percent to 208 percent, as seen in table 2.²³

Table 2: The 23 Civilian Chief Financial Officers Act of 1990 Agencies' Reported Spending on Information Security for Fiscal Year 2018

Agency	Total IT spending (dollars in millions)	Total IT security spending (dollars in millions) ^a	Percent of IT spending used for IT security
Department of Agriculture	1,610	262	16
Department of Commerce	2,745	350	13
Department of Education	692	104	15
Department of Energy	1,842	448	24
Department of Health and Human Services	6,265	359	6
Department of Homeland Security	7,424	1,859	25
Department of Housing and Urban Development	281	15	5
Department of the Interior	1,131	88	8
Department of Justice	2,903	821	28
Department of Labor	732	93	13
Department of State	2,246	362	16
Department of Transportation	3,360	185	6
Department of the Treasury	4,545	445	10
Department of Veteran Affairs	4,785	386	8
Environmental Protection Agency	407	21	5

²³According to the *President's IT Budget for Fiscal Year 2020*, the agency reported IT security spending amount may include cybersecurity-related spending that was not dedicated to the protection of their networks. Instead, the spending amounts reported may represent spending for the broader cybersecurity mission of the agency.

Agency	Total IT spending (dollars in millions)	Total IT security spending (dollars in millions) ^a	Percent of IT spending used for IT security
General Services Administration	664	72	11
National Science Foundation	119	247	208
National Aeronautics and Space Administration	2,335	171	7
Nuclear Regulatory Commission	153	25	16
Office of Personnel Management	141	38	27
Small Business Administration	112	9	8
Social Security Administration	1,923	167	9
U.S. Agency for International Development	195	44	23
Total	46,610	6,571	14

Source: GAO analysis of budget and spending data provided in the President's IT Budget for Fiscal Year 2020 and IT Dashboard. | GAO-19-545

^aFor some agencies with missions related to cybersecurity research and oversight (e.g., the National Science Foundation and the Department of Homeland Security), the agency-reported information security spending amounts may include spending that was not dedicated to the protection of their own networks, but related to their broader cybersecurity mission.

Security Control Deficiencies Reported at Selected Agencies Indicate Ineffective Information Security Policies and Practices

Information security reports issued by GAO, inspectors general, and CIOs indicate that information security policies and practices of the agencies we reviewed are ineffective. Specifically, information security evaluation reports that we and agency inspectors general issued during fiscal year 2018 showed that most of the 16 selected agencies did not consistently or effectively implement policies or practices related to the core security functions of the cybersecurity framework. In addition, most of these selected agencies had deficiencies in implementing the eight elements of an information security program, as defined by FISMA. Also, inspectors general reported that most of the 24 CFO Act agencies did not have effective information security programs and were not effectively implementing security controls over financial systems during fiscal year 2018. Further, agency CIOs reported that most of the 23 civilian CFO Act agencies had not met targets for implementing cyber capabilities to reduce risk.

Most of the 16 Selected Agencies Exhibited Deficiencies in All Cybersecurity Framework Core Security Functions

FISMA requires agencies and their inspectors general to report on the adequacy and effectiveness of information security policies, procedures, and practices. To facilitate meeting this reporting requirement, CIGIE, in collaboration with OMB and DHS, developed metrics that agency inspectors general are to use to report on eight security domains²⁴ that align with the five core security functions—*Identify, Protect, Detect, Respond, and Recover*—of the NIST cybersecurity framework. Table 3 illustrates how the inspector general reporting domains are related to the core security functions.

Table 3: Cybersecurity Framework Core Security Functions’ Relation to the Inspector General (IG) Reporting Domains

Core security functions	IG reporting domains
Identify	Risk management
Protect	Configuration management Identity and access management Data protection and privacy Security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

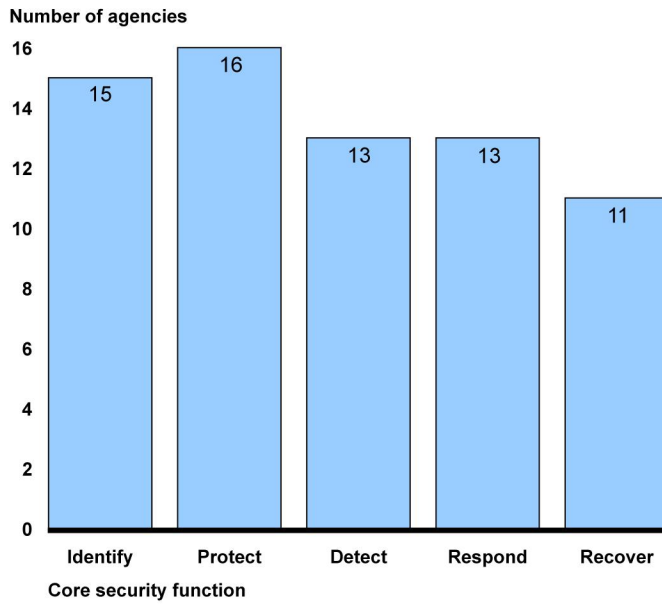
Source: FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.0.1 May 24, 2018. | GAO-19-545

Most of the 16 agencies that we reviewed had deficiencies in implementing policies and practices related to the cybersecurity framework core security functions and related domains during fiscal year

²⁴The inspector general reporting metrics identify eight domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

2018.²⁵ Figure 3 shows the number of agencies with reported deficiencies in each of the framework’s core security functions.

Figure 3: Number of 16 Selected Agencies with Deficiencies in Information Security Policies, Procedures, and Practices, by Core Security Function



Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices of 16 agencies for fiscal year 2018. | GAO-19-545

Data table for Figure 3: Number of 16 Selected Agencies with Deficiencies in Information Security Policies, Procedures, and Practices, by Core Security Function

Core security function	Number of agencies
Identify	15
Protect	16
Detect	13
Respond	12
Recover	11

²⁵The 16 agencies reviewed were the Departments of the Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Selected Agencies Did Not Adequately Implement Activities to Identify Cybersecurity Risk

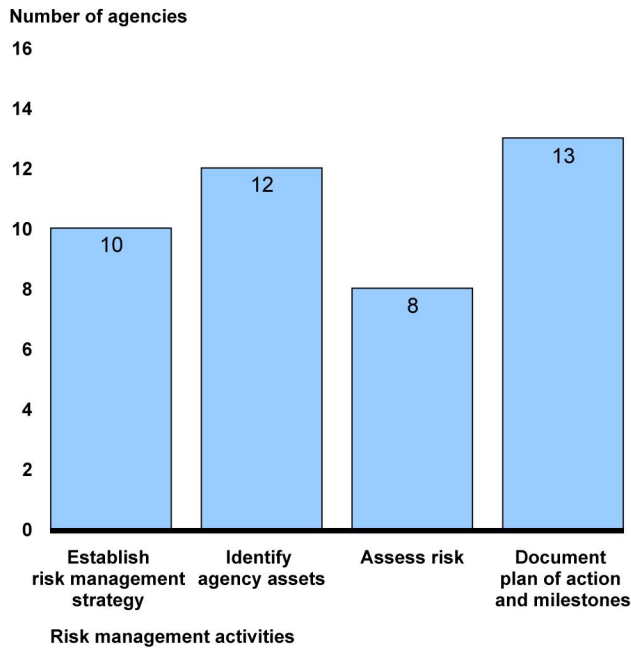
The *Identify* core security function includes the key process of risk management. NIST defines risk management as the process of identifying and assessing risk, and taking steps to reduce those risks to an acceptable level. NIST guidance specifies activities that agencies should implement to effectively identify and manage cybersecurity risks, including:

- establishing a risk management strategy that includes a determination of risk tolerance;
- identifying assets that require protection;
- assessing risk; and
- documenting plans of action and milestones (POA&Ms) to mitigate known deficiencies.²⁶

Fifteen of the 16 selected agencies had deficiencies in activities associated with identifying risks. Figure 4 illustrates the number of selected agencies that had deficiencies in each of the activities.

²⁶National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37 Revision 2 (Gaithersburg, MD: December 2018).

Figure 4: Number of 16 Selected Agencies with Deficiencies in Risk Management Activities



Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices for fiscal year 2018. | GAO-19-545

Data table for Figure 4: Number of 16 Selected Agencies with Deficiencies in Risk Management Activities

Risk management control	Number of agencies
Establish risk management strategy	10
Identify agency assets	12
Assess risk	8
Document plan of action and milestones	13

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Establishment of a Risk Management Strategy

Risk management strategies include strategic-level decisions and considerations for how senior leaders and executives are to manage risk to organizational operations and assets, individuals, other organizations,

and the nation.²⁷ GAO and inspectors general reports identified that 10 of the 16 selected agencies had deficiencies in developing, documenting, or implementing a risk management strategy. Specifically, nine of the 10 agencies had not developed or documented an enterprise-wide risk management strategy or process. Another agency had developed an enterprise risk management strategy but had not implemented it consistently across the agency.

Without developing or documenting a risk management strategy, agencies lack clear guidance to help them make informed decisions for managing risk. Further, if agencies do not consistently implement a risk management strategy, they can potentially hinder their efforts to effectively identify and manage risk.

Identification of Agency Assets

FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under the control of the agency to support risk management activities. Further, NIST Special Publication 800-53 states that centralized inventories of hardware, software, and firmware assets should be maintained to ensure proper accountability of those assets.²⁸ These inventories also should be current, complete, and accurate to ensure proper accountability.

Twelve of the 16 selected agencies did not fully identify or account for their major information systems or information technology assets. One agency did not maintain a comprehensive and accurate inventory of information systems and two other agencies did not maintain a current inventory of hardware and software assets. Nine additional agencies maintained neither a comprehensive and accurate inventory of information systems nor a current inventory of software and hardware assets. If agencies do not maintain comprehensive, accurate, or up-to-date inventories of information systems or hardware and software assets, agencies cannot ensure the protection of all assets within their networks.

²⁷National Institute of Standards and Technology, Special Publication 800-37, Revision 2.

²⁸National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, MD: April 2013).

Assessment of Risks

FISMA requires agencies to develop, document, and implement an agency-wide information security program that includes periodic risk assessments. According to NIST,²⁹ these assessments are to address potential adverse impacts resulting from the operation and use of information systems and the information those systems process, store and transmit.

Eight of the 16 selected agencies exhibited deficiencies in conducting risk assessments. Of the eight agencies that had deficiencies, four did not consistently perform risk assessments of their information systems; three did not fully update risk assessments subsequent to system changes; and one did not conduct a risk assessment supporting the agency's decision to allocate resources to support mission and business processes. Without a sufficient process for conducting periodic risk assessments, agencies cannot determine, or appropriately respond to, risks to the information systems supporting the organization.

Documentation of Plans of Action and Milestones

FISMA requires agency information security programs to include a process for planning, implementing, evaluating, and documenting remedial action to address deficiencies in information system policies, procedures, and practices. In addition, NIST's risk management framework states that agencies should implement a consistent process for developing POA&Ms using a prioritized approach to risk mitigation that is guided by a risk assessment. Further, documentation of POA&Ms should also be updated to reflect the current status of the deficiencies and, after remedial actions have been completed, agencies should test the actions to determine if they effectively addressed the deficiencies.

Thirteen of the 16 selected agencies had deficiencies in their POA&M processes. Specifically, five agencies did not have an effective process for remediating vulnerabilities in a timely manner; seven other agencies did not adequately document or track the status of POA&Ms; and another agency did not assess the root cause of identified deficiencies to prioritize corrective actions based on the highest areas of risks. Additionally, one of

²⁹National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1, (Gaithersburg, MD: September 2012).

the agencies that did not adequately document POA&Ms also did not have sufficient evidence to conclude that deficiencies were corrected even though the agency validated the remediation of the deficiency through its closure verification process.

Without sufficiently documenting POA&Ms, agencies may not sufficiently remediate information security deficiencies in a timely manner, exposing their systems to increased risks that nefarious actors will exploit the deficiencies to gain unauthorized access to information resources.

All Selected Agencies Had Deficiencies in Developing and Implementing Appropriate Safeguards to Protect Cyber Assets

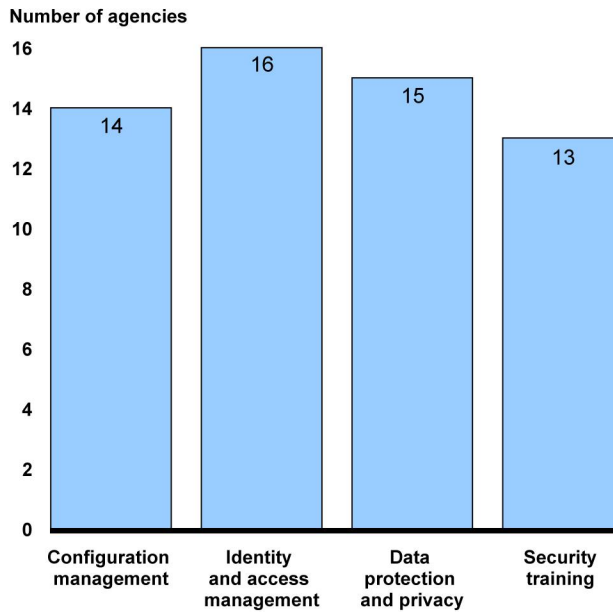
Agencies are to implement appropriate safeguards associated with the following four security domains that align with the *Protect* core security function:

- configuration management;³⁰
- identity and access management;
- data protection and privacy; and
- security training.

Each of the 16 selected agencies was deficient in developing and implementing appropriate safeguards to protect agency systems and networks. As shown in figure 5, most of the selected agencies had deficiencies in each of the four domains.

³⁰NIST defines configuration management as the collection of activities focused on establishing and maintaining the integrity of products and systems through control of processes for initializing, changing, and monitoring the configurations of those products and systems.

Figure 5: Number of 16 Selected Agencies with Deficiencies in the Security Domains Aligned to the Protect Core Security Function



Security domains aligned to the *protect* core security function

Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices for fiscal year 2018. | GAO-19-545

Data table for Figure 5: Number of 16 Selected Agencies with Deficiencies in the Security Domains Aligned to the Protect Core Security Function

Security domains aligned to the Protect core security function	Number of agencies
Configuration management	14
Identity and access management	16
Data protection and privacy	15
Security training	13

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Configuration Management

NIST guidelines specify that agencies are to develop, implement, and maintain a baseline configuration;³¹ control changes to system configurations; and securely configure information systems.³² However, 14 of the selected 16 agencies reported weaknesses in one or more of these configuration management activities.

Of the 14 agencies, nine had weaknesses in developing, maintaining, and implementing a baseline configuration for their information systems. For example, four agencies did not develop a baseline configuration for all systems or network devices. In addition, two agencies did not review or approve their baseline configurations. Further, three agencies did not consistently implement their baseline configurations. If agencies do not develop, maintain, or implement a current and comprehensive baseline of information systems and network devices, agencies cannot validate configuration information for accuracy, thereby hindering them from controlling changes made to a system.

Eleven agencies did not effectively or consistently control changes to the configuration of their information systems. Properly controlling system changes can help agencies to ensure that changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation. However, six of the 11 agencies did not properly approve or test changes before they were implemented; four other agencies did not consistently implement change control activities across their organization or their information systems; and one other agency did not consistently ensure accountability and responsibility for individuals performing configuration management activities.

In addition, 12 agencies did not securely configure their information systems. NIST specifies that agencies should apply software patches in a timely manner, use vendor-supported software, apply secure configuration settings, and limit system functionality to least level needed to meet organizational requirements.³³ However, of the 12 agencies that

³¹A baseline configuration is a set of specifications for a system, or system components, which have been reviewed and agreed upon.

³²National Institute of Standards and Technology, *Guide for Security-focused Configuration Management of Information Systems*, Special Publication 800-128 (Gaithersburg, MD: August 2011).

³³ National Institute of Standards and Technology, Special Publication 800-128.

had deficiencies in implementing secure configurations, nine did not implement patches to address vulnerabilities or use up-to-date software that was supported by a vendor. Ten agencies also did not apply secure configuration settings to effectively enable security and facilitate the management of risk, while two agencies did not implement controls for limiting system functionality. As a result, these agencies cannot validate configuration information for their information systems and assets, detect or prevent unauthorized changes to information system resources, or provide a reasonable assurance that systems are configured and operating securely and as intended.

Identity and Access Management

Access controls are intended to limit or detect inappropriate access to computer resources to protect them from unauthorized modification, loss, and disclosure. Such controls include logical controls that require users to validate their identity and limit the files and other resources that those validated users can access and the actions they can execute.

All 16 agencies that we reviewed had deficiencies in effectively implementing one or more controls associated with the identity and access management domain during fiscal year 2018. Fifteen of the 16 selected agencies did not adequately control user's access to information systems and the information residing on them. For example, seven agencies did not appropriately authorize or approve system access before access was granted, and eight agencies did not perform user access reviews to ensure that they complied with account management policy.

Additionally, 11 of the 16 agencies did not properly identify and validate information system users, which involve enforcing strong passwords and requiring passwords to be changed periodically. In addition, 11 of the 16 agencies had deficiencies in implementing access management to ensure separation of duties, or segregating work responsibilities so that one individual does not control all critical stages of a process. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain.

Data Protection and Privacy

According to NIST guidance on security and privacy controls, agencies should protect data at rest and in transit on their network through implementation of cryptography and other technologies to achieve confidentiality and integrity protections over that data.³⁴ In addition, NIST's guidance states that agencies should implement contingency strategies, such as conducting backups of information systems and having alternate processing and storage sites to protect data from loss during an interruption and to resume activities after an interruption.³⁵ Further, NIST guidance states that agencies should develop privacy policies, procedures, and guidance for safeguarding the collection, access, use, dissemination, and storage of personally identifiable information that supports a privacy program.³⁶

However, 15 of the 16 selected agencies did not effectively implement controls to protect data and ensure its privacy during fiscal year 2018. Specifically, eight of the 16 agencies did not adequately implement controls for protecting information at rest and four agencies did not adequately implement controls for ensuring the integrity and confidentiality of data in transit. In addition, five of the 16 agencies did not conduct backups of information systems and five agencies did not use alternate processing sites to retrieve backups or resume essential mission/business functions. Further, the inspectors general for 14 of the 16 agencies reported that their respective agency did not effectively document or implement policies and procedures supporting the agency's privacy program. If agencies do not effectively implement controls to protect data and ensure its privacy, agencies may be hindered in limiting or containing the impact of a potential cybersecurity event.

Security Training

FISMA requires agency information security programs to include security awareness training to inform personnel of information security risks

³⁴National Institute of Standards and Technology, Special Publication 800-53, Rev 4.

³⁵National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, Rev. 1 (Gaithersburg, MD: May 2010).

³⁶National Institute of Standards and Technology, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Internal Report (NISTIR) 8062 (Gaithersburg, MD: January 2017).

associated with their activities and responsibilities in complying with agency policies and procedures intended to reduce risk. In addition, FISMA requires agencies to provide role-based training to personnel with significant responsibilities for information security. Further, NIST guidance on building an IT security awareness and training program states that an awareness and training program is the means to communicate information that users need to support the mission of the organization, and security requirements across the agency.³⁷

Most of the selected agencies exhibited deficiencies in implementing a security training program during fiscal year 2018. Only three of the 16 selected agencies effectively implemented elements of a security training program. Of the 13 agencies that had deficiencies, 12 did not ensure that personnel received security awareness training and 10 did not ensure that personnel with significant responsibilities for information security received role-based training, including nine agencies that were deficient in providing both types of training. As a result, these agencies risk having employees or contractors that are ill-prepared to protect systems, and risk inadvertently or intentionally compromising security.

Most of the Selected Agencies Had Not Effectively Developed or Implemented Controls to Detect Cyber Events and Vulnerabilities

Agencies are to develop and implement controls to *Detect* cyber events and vulnerabilities. FISMA requires agencies to develop, document, and implement an agency-wide information security program that includes periodic testing and evaluation of effectiveness and procedures for detecting security incidents. NIST guidelines define these and other activities as part of information security continuous monitoring,³⁸ including:

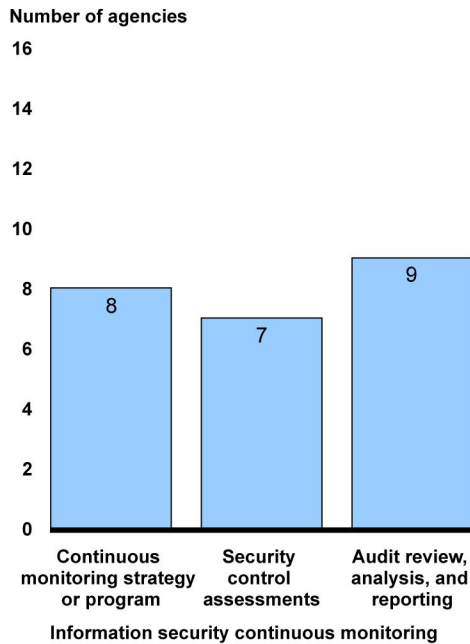
³⁷National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50 (Gaithersburg, MD: October 2003).

³⁸Information security continuous monitoring is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, NIST Special Publication 800-137 (Gaithersburg, MD: September 2011).

- defining an information security continuous monitoring strategy and implementing an information security continuous monitoring program in accordance with that strategy;
- assessing and reporting on the effectiveness of all implemented security controls; and
- collecting, correlating, and analyzing security related information obtained through information system auditing.

However, as shown in figure 6, agencies exhibited deficiencies in activities associated with information security continuous monitoring.

Figure 6: Number of 16 Selected Agencies with Deficiencies in Information Security Continuous Monitoring



Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-19-545

Data table for Figure 6: Number of 16 Selected Agencies with Deficiencies in Information Security Continuous Monitoring

Information security continuous monitoring	Number of agencies
Continuous monitoring	8
Security control assessments	7
Audit review, analysis, and reporting	9

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Continuous Monitoring Strategy and Program

NIST's guidance on information security continuous monitoring states that defining an information security continuous monitoring strategy and developing an information security continuous monitoring program are the first two steps in creating, implementing, and maintaining information security continuous monitoring.³⁹ In addition, agencies should implement the information security continuous monitoring program in accordance with the defined strategy.

However, half of the 16 selected agencies did not develop an information security continuous monitoring strategy or program, or implement the information security continuous monitoring program. Specifically, five of the agencies did not fully develop an information security continuous monitoring strategy or program. In addition, while three agencies had developed, or made organizational changes to create a foundation for, an information security continuous monitoring strategy, those agencies did not consistently or effectively implement the strategy. Without a well-designed and implemented information security continuous monitoring strategy, agencies could be hindered in assuring ongoing situational awareness of information security, vulnerabilities, and threats.

Security Control Assessments

As stated above, FISMA requires agencies to include periodic testing and evaluation of information security policies, procedures, and practices in agency-wide information security programs. Security control assessments determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system requirements.

Most agencies assessed the controls implemented on their systems. However, seven agencies did not consistently perform system control assessments to ensure that the controls were operating effectively, or as

³⁹National Institute of Standards and Technology, Special Publication 800-137.

intended. Further, seven agencies had not completed or implemented other activities in their security assessment and authorization process that assists agencies with ensuring that appropriate controls are implemented on an information system and that the system is authorized to operate. If agencies do not perform consistent testing of information security controls, they cannot determine that implemented controls are appropriately designed or operating effectively.

Audit Review, Analysis, and Reporting

According to NIST guidance on log management, routine log analysis is beneficial to identifying security incidents, policy violations, fraudulent activity, and operational problems. As a result, log analysis supports information security continuous monitoring capabilities.

However, more than half of the 16 selected agencies did not review, analyze, and report auditable events from audit logs. For example, nine agencies did not implement audit log review capabilities on their information systems. Without reviewing, analyzing, and reporting audit logs, agencies limit their ability to identify unauthorized, unusual, or sensitive access activity on their networks.

Most of the Selected Agencies Exhibited Deficiencies in Developing and Implementing Controls to Respond to Detected Cyber Intrusions

Agencies should have policies and practices in place to *Respond* to detected incidents. FISMA requires agency information security programs to include procedures for responding to security incidents in order to mitigate risks associated with such incidents before substantial damage is done. According to NIST, incident response involves rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.⁴⁰ An effective incident response process includes, for example:

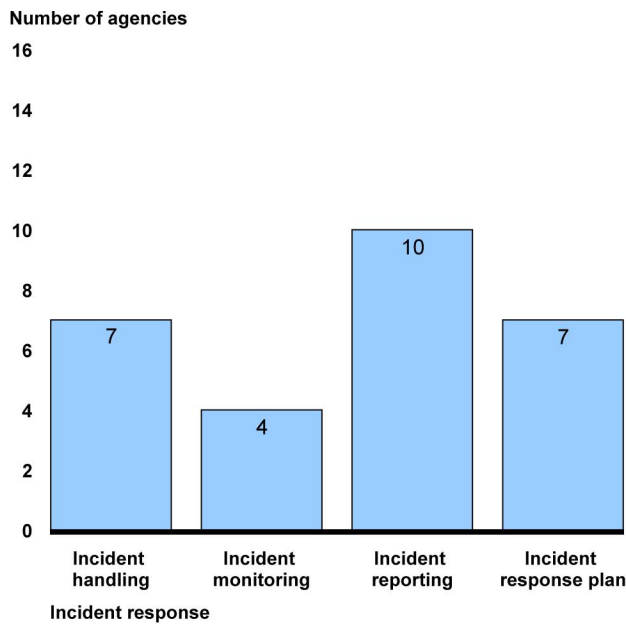
- an incident handling capability that incorporates lessons learned from ongoing incident handling activities;

⁴⁰National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2 (Gaithersburg, MD: August 2012).

- the monitoring of incidents through documentation that includes pertinent information necessary for forensics, evaluating incident details, trends, and handling;
- the timely reporting of incidents with sufficient detail to allow analysis; and
- an incident response plan.

Most of the 16 selected agencies had deficiencies in at least one of the activities associated with incident response processes, as shown in figure 7.

Figure 7: Number of 16 Selected Agencies with Deficiencies in Incident Response



Source: GAO analysis of agency, inspectors general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-19-545

Data table for Figure 7: Number of 16 Selected Agencies with Deficiencies in Incident Response

Incident response	Number of agencies
Incident handling	7
Incident monitoring	4
Incident reporting	10
Incident response plan	7

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

Incident Handling

According to NIST, agencies should have the ability to detect and analyze security incidents in order to minimize loss and destruction and mitigate the weaknesses that were exploited.⁴¹ In addition, agencies should incorporate lessons learned from an incident to improve existing security controls and practices.

Most of the selected agencies did not report deficiencies associated with their incident handling capability, including the ability to analyze and respond to security incidents and incorporate lessons learned. However, seven agencies did not adequately implement capabilities to analyze and respond to security incidents. In addition, one of the seven agencies did not use lessons learned from prior incidents to improve incident handling. Without an effective incident handling capability, agencies have limited ability to detect and analyze security incidents to minimize destruction and mitigate exploited vulnerabilities.

Incident Monitoring

According to NIST, agencies should monitor and document security incidents with sufficient detail in order to effectively respond to and mitigate the risks associated with the incident.⁴² Doing so enables agencies to analyze security incidents, understand the impact of the incident, and perform analysis to identify trends and indicators of attack.

Inspectors general for 12 of the 16 selected agencies did not identify deficiencies related to monitoring detected incidents. However, four agencies did not effectively monitor incidents. For example, one agency did not consistently document incidents detected and another agency had not implemented an automated enterprise tool for monitoring incidents. If agencies do not effectively implement incident monitoring processes, they

⁴¹National Institute of Standards and Technology, Special Publication 800-61, Revision 2.

⁴²National Institute of Standards and Technology, Special Publication 800-61, Revision 2.

hinder their ability to adequately analyze and respond to security incidents.

Incident Reporting

FISMA requires agencies to develop, document, and implement an agency-wide information security program that includes procedures for reporting security incidents to US-CERT. In addition, NIST guidance states that agencies should have specific incident reporting requirements for reporting suspected security incidents to an internal incident reporting organization.⁴³

However, 10 agencies had deficiencies in their implementation of incident reporting. While only two agencies did not clearly define incident reporting requirements, eight agencies did not effectively implement those requirements. For example, these agencies did not consistently categorize incidents or ensure timely reporting of incidents to US-CERT and internal reporting organizations. If agencies do not consistently categorize or report incidents in an accurate and timely manner, they cannot effectively respond to incidents because they may lack effective situational awareness in order to appropriately respond to incidents.

Incident Response Plan

Incident response plans are an important element to ensuring that incident response is performed effectively, efficiently, and consistently throughout the agency. Among other things, NIST guidance states that incident response plans should provide a roadmap for implementing an incident response capability, describe metrics for measuring the incident response capability, and be approved.⁴⁴

Inspectors general for nine of the selected agencies did not report deficiencies related to incident response plans. However, seven agencies did not fully develop or monitor the effectiveness of their incident response plans. Specifically, five agencies had incident response plans that did not fully define requirements for implementing their incident response capability or were not approved. In addition, the other two agencies did not use performance metrics to verify the effectiveness of

⁴³National Institute of Standards and Technology, Special Publication 800-61, Revision 2.

⁴⁴National Institute of Standards and Technology, Special Publication 800-61, Revision 2.

their incident response plan. Without an effective and comprehensive incident response plan, agencies cannot implement a coordinated approach to incident response.

More Than Half of the Selected Agencies Had Not Adequately Developed or Implemented Practices to Recover from Cyber Events

Agencies should be able to *Recover* from cyber events. FISMA requires agencies to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. NIST defines contingency planning as a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning is significant to protecting electronically maintained data and an agency's ability to process and retrieve data during and after a cyber intrusion. According to NIST, agencies should develop and document a comprehensive contingency plan or suite of related plans for restoring capabilities during and after a cyber event.⁴⁵ The suite of related plans should include a disaster recovery plan and business impact analysis.⁴⁶

However, 11 of the 16 selected agencies did not sufficiently plan for recovering system operations after an interruption. Specifically, these 11 agencies did not consistently develop contingency plans, to include disaster recovery plans, or other associated documentation, such as business impact analyses for all of their information systems. In addition, one agency did not define how the agency is to process and retrieve data during and after an interruption. Without an effective contingency planning process, agencies are exposed to the risk of interruptions to information system operations and disruption to their mission and business processes.

⁴⁵National Institute of Standards and Technology, Special Publication 800-34, Revision 1.

⁴⁶Business impact analysis should be conducted to (1) identify critical IT resources, (2) identify outage impact and allowable outage times, and (3) identify recovery priorities.

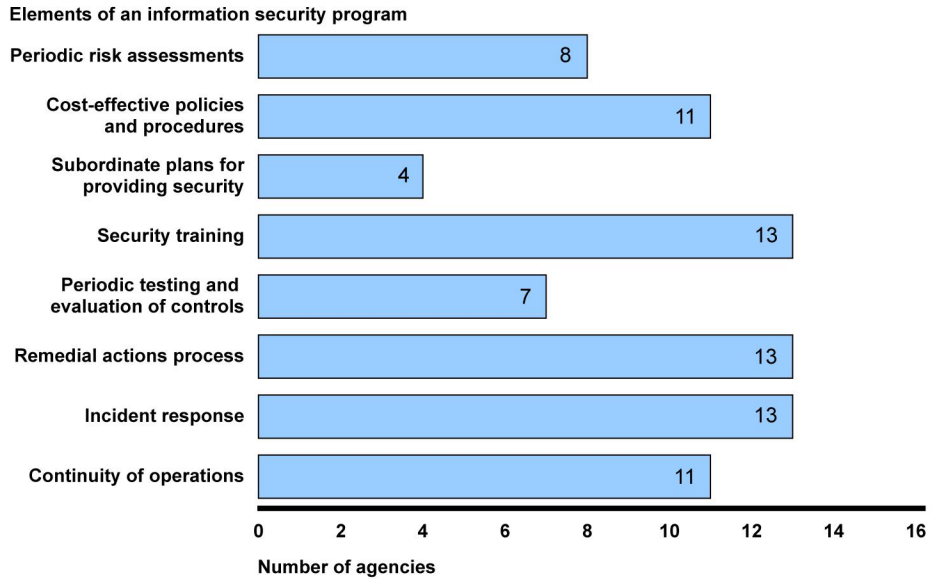
Most of the 16 Selected Agencies Exhibited Deficiencies in Implementing Elements of an Information Security Program

Controls associated with the five core security functions are related to elements of agencies' information security programs. FISMA requires each agency to develop, document, and implement an information security program that includes the following eight elements:

1. periodic assessments of the risk;
2. cost-effective policies and procedures that reduce risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each system, and ensure compliance with applicable requirements;
3. subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
4. security awareness training and training for personnel with significant responsibilities for information security;
5. periodic testing and evaluation of the effectiveness of security policies, procedures, and practices;
6. a process for planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies;
7. procedures for detecting, reporting, and responding to security incidents; and
8. plans and procedures to ensure continuity of operations for information systems.

As discussed earlier in this report, most of the 16 selected agencies had deficiencies related to implementing the eight elements of an agency-wide information security program. Figure 8 shows the number of selected agencies with deficiencies in implementing the eight elements of an agency-wide information security program.

Figure 8: Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Agency-wide Information Security Program, as Required by the *Federal Information Security Modernization Act of 2014*



Source: GAO analysis of agency, inspector general, and GAO reports on the information security policies and practices at 16 agencies for fiscal year 2018. | GAO-19-545

Data table for Figure 8: Number of 16 Selected Agencies with Deficiencies in the Eight Elements of an Agency-wide Information Security Program, as Required by the *Federal Information Security Modernization Act of 2014*

Elements of an information security program	Number of agencies
Periodic risk assessments	8
Cost-effective policies and procedures	11
Subordinate plans for providing security	4
Security training	13
Periodic testing and evaluation of effectiveness	7
Remedial actions process	13
Incident response	13
Continuity of operations	11

Note: The 16 selected agencies are the Departments of Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; and the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration.

For example, of the 16 selected agencies:

- Eight agencies did not effectively assess risk;
- 11 agencies did not have policies to ensure that CIOs carried out their role as it relates to information security;
- Four agencies developed incomplete system security plans;
- 13 agencies did not ensure that personnel received security awareness training, or that personnel with security responsibilities received role-based security training;
- Seven agencies did not consistently perform control assessments to ensure that the controls were operating effectively, or as intended;
- 13 agencies did not effectively implement their POA&M process to address information security deficiencies;
- 13 agencies did not adequately detect or respond to incidents; and
- 11 agencies did not comprehensively develop plans to ensure the continuity of its operations.

We and inspectors general have made numerous recommendations aimed at improving information security programs and practices over the years. Until these agencies take action to address deficiencies in implementing the eight elements of an agency-wide information security program, they lack assurance that their information systems and networks are protected from inadvertent or malicious activity.

Inspectors General Determined That the 24 CFO Act Agencies Generally Did Not Have Effective Information Security Policies and Practices

Inspectors general determined that few agencies covered by the *CFO Act of 1990* had effective agency-wide information security programs during fiscal year 2018. Further, in agency financial statement audit reports for fiscal year 2018, inspectors general reported that they continued to identify significant deficiencies in information security controls over financial systems. As a result, inspectors general reported material weaknesses or significant deficiencies in internal control over financial reporting for fiscal year 2018.

Inspectors General Indicate That Few CFO Act Agencies had Effective Information Security Programs

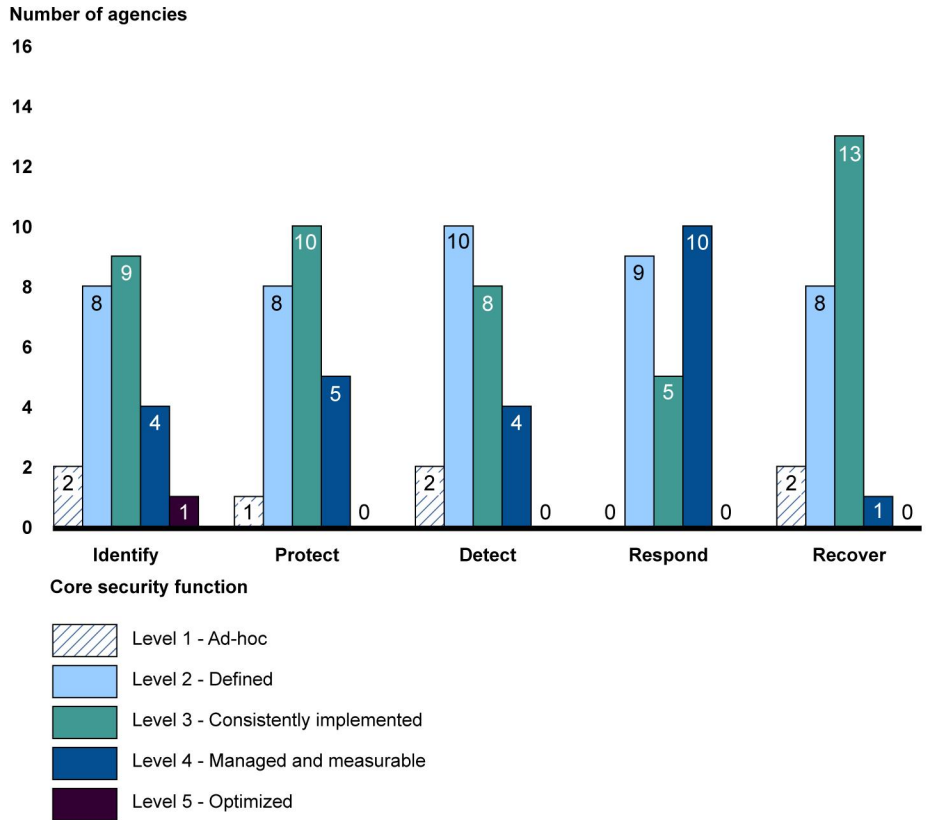
FISMA requires inspectors general to determine the effectiveness of their respective agencies' information security programs. To do so, OMB

instructed inspectors general to provide a maturity rating for agency information security policies, procedures, and practices related to the five core security functions established in the NIST cybersecurity framework, as well as for the agency-wide information security program.⁴⁷

For fiscal year 2018, the inspectors general for only six of the 24 CFO Act agencies reported that their agencies had an effective agency-wide information security program. However, the remaining 18 agencies were reported as having ineffective information security programs. When considering each of the five core security functions, most inspectors general reported that their agency was at Level 3 (consistently implemented) for the *Identify*, *Protect*, and *Recover* functions; at Level 2 (defined) for the *Detect* function; and at Level 4 (managed and measurable) for the *Respond* function, as shown in figure 9.

⁴⁷ *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.0.1 (Washington, D.C.: May 24, 2018).

Figure 9: Inspector General Ratings of 24 *Chief Financial Officers Act of 1990* Agencies' Information Security Policies, Procedures, and Practices Related to the Cybersecurity Framework Core Security Functions



Source: GAO analysis of agency fiscal year 2018 Federal Information Security Modernization Act reports. | GAO 19-545

Data table for Figure 9: Inspector General Ratings of 24 *Chief Financial Officers Act of 1990* Agencies' Information Security Policies, Procedures, and Practices Related to the Cybersecurity Framework Core Security Functions

	Level 1	Level 2	Level 3	Level 4	Level 5
Identify	2	8	9	4	1
Protect	1	8	10	5	0
Detect	2	10	8	4	0
Respond	0	9	5	10	0
Recover	2	8	13	1	0

Note: The 24 *Chief Financial Officers Act of 1990* 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.

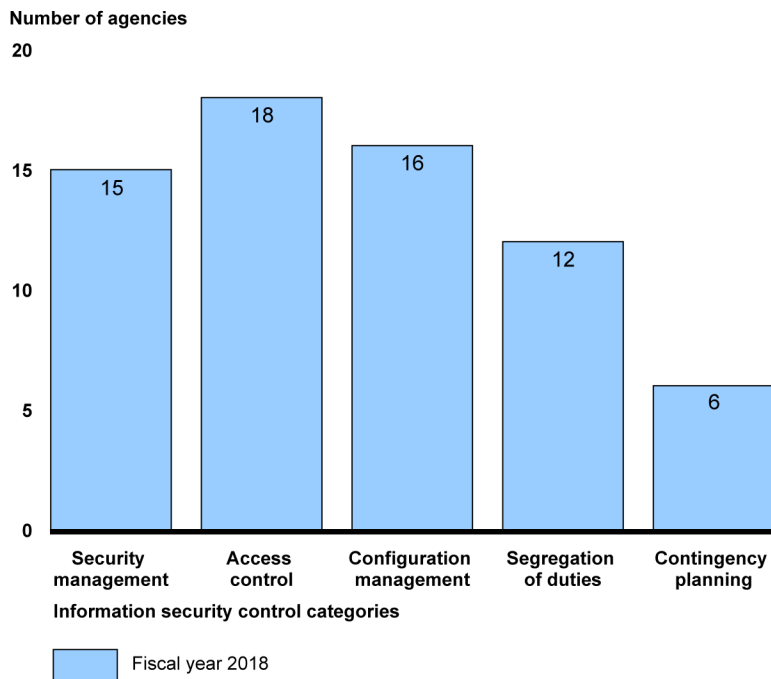
Inspectors General Continued to Identify Significant Security Control Deficiencies in Controls over Financial Reporting at Most CFO Act Agencies

Agency inspectors general report on the effectiveness of agencies' information security controls as part of the annual audits of the agencies' financial statements. The reports resulting from these audits include a description of information security control deficiencies related to the five major control categories defined by the *Federal Information System Controls Audit Manual* (FISCAM)—security management, access controls, configuration management, segregation of duties, and contingency planning.⁴⁸

For fiscal year 2018, inspectors general identified information security control deficiencies related to most of the FISCAM general control categories for most of the 24 CFO Act agencies as shown in figure 10.

⁴⁸FISCAM is GAO's audit methodology for performing information system control audits in accordance with generally acceptable government auditing standards. The five general control categories defined by this manual are: (1) security management controls that provide a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended; (2) access controls that limit or detect access to computer resources, thereby protecting them against unauthorized modification, loss, and disclosure; (3) configuration management controls that prevent unauthorized changes to information system resources and to assure that software is current and known vulnerabilities are patched; (4) segregation of duties controls that prevent an individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; and (5) contingency planning controls that help avoid significant disruptions in computer-dependent operations. See GAO, *Federal Information System Controls Audit Manual* (FISCAM), [GAO-09-232G](#) (Washington, D.C.: February 2009).

Figure 10: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018



Source: GAO analysis of agency financial reports for fiscal year 2018. | GAO-19-545

Data table for Figure 10: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018

	Number of Agencies
Security Management	15
Access Control	18
Configuration Management	16
Segregation of Duties	12
Contingency Planning	6

Note: The 24 Chief Financial Officers Act of 1990 agencies are the Departments of the 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.

Overall, inspectors general for the 24 CFO Act agencies continued to report deficiencies in agencies information security practices for fiscal

year 2018. Specifically, during that time, 18 inspectors general designated information security as either a material weakness (6) or significant deficiency (12) in internal control over financial reporting systems for their agency.⁴⁹ Further, inspectors general at 21 of the 24 agencies cited information security as a major management challenge for their agency for fiscal year 2018.

Most of the 23 Civilian CFO Act Agencies Reported Not Fully Meeting Targets for Implementing Cyber Capabilities to Mitigate Risks

OMB, in its fiscal year CIO reporting metrics, directed CIOs to assess their agencies' progress toward achieving outcomes that strengthen federal cybersecurity. To do this, CIOs evaluated their agency's performance in reaching targets for meeting key milestones of the current administration's IT Modernization Cross-Agency Priority (CAP) goal. This CAP goal includes a cybersecurity initiative to mitigate the impact of risks to federal agencies' data, systems, and networks by implementing cutting edge cybersecurity capabilities.

The CAP goal's cybersecurity initiative has three strategies that include key milestones with specific implementation targets, most of which are expected to be met by the end of fiscal year 2020. Table 4 shows the key milestones and targets related to the three strategies of the IT Modernization CAP goal's cybersecurity initiative, as well as how many agencies were meeting the targets for each of the milestones.

⁴⁹A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatement on a timely basis.

Table 4: Number of 23 Civilian Chief Financial Officers Act of 1990 Agencies Meeting Cross-Agency Priority Goal Targets for 10 Key Milestones

Strategy	Key milestone	Target	Number of agencies reported meeting targets
Manage asset security by implementing capabilities that provide observational, analytical, and diagnostic data of an agency's cybersecurity.	Software asset management	95% of software assets are covered by a whitelisting capability. ^a	10
	Hardware asset management	95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.	16
	Authorization management	100% of high and moderate impact systems are covered by a valid security authorization to operate.	14
	Mobile device management	95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	19
Limit personnel access by implementing credential and access management capabilities that ensure users only have access to the resources necessary for their job function.	Privileged network access management	100% of privileged users are required to use a personal identity verification (PIV) ^b card or authenticator assurance level 3 (AAL3) ^c multifactor authentication method to access the agency's network.	18
	High-value asset access management	90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	14
	Automated access management	95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	15
Protect networks and data by implementing advanced network and data protection capabilities to protect agency networks and sensitive government and citizen data.	Intrusion detection and prevention	At least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90%, and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.	7
	Exfiltration and enhanced defenses	At least 3 of 4 exfiltration and enhanced defenses metrics have met an implementation target of at least 90%.	23
	Data protection	At least 4 of 6 data protection metrics have met an implementation target of at least 90%.	16

Source: GAO analysis of Fiscal Year 2018 Chief Information Officer Federal Information Security Modernization Act of 2014 Reporting Metrics | GAO-19-545

^aWhitelisting is a process used to identify (1) software programs that are authorized to execute on an information system or (2) authorized websites.

^bPersonal identity verification card is a physical artifact that contains stored identity credentials for the person it was issued to, so that the identity of the individual can be verified against the stored credentials by another person or an automated process.

^cAuthenticator assurance level 3 uses a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.

Overall, only two of the civilian 23 CFO Act agencies met all 10 targets for the cybersecurity initiative of the IT Modernization CAP goal, during fiscal year 2018. Whereas, 10 agencies met seven to nine of the targets and the remaining 11 agencies met six or fewer targets. More specifically, by strategy area,

- Seven agencies met all four targets for the manage asset security strategy.
- Eight agencies met all three targets for the limit personnel security strategy.
- Seven agencies met all three targets for the protect networks and data strategy.

OMB, DHS, and NIST Acted to Fulfill Their FISMA-defined Roles, but Shortcomings Exist in Government-wide Efforts Intended to Improve Federal Information Security

OMB, DHS, and NIST have ongoing and planned initiatives to support FISMA's implementation across the federal government. Specifically, OMB developed and oversaw the implementation of information security policies, procedures, and guidelines over the past 2 years. In addition, DHS oversaw and assisted government efforts that were intended to provide adequate, risk-based, cost-effective cybersecurity. Further, NIST continued to provide guidance to federal agencies to improve information security across the government.

However, beyond fiscal year 2016, OMB held CyberStat meetings at significantly fewer agencies. These meetings are intended to help ensure effective implementation of information security policies and practices. In addition, OMB's guidance to agencies for preparing their fiscal year 2018 FISMA report does not sufficiently address FISMA's requirement for developing subordinate plans for providing adequate information security for networks, facilities, and information systems.

OMB Provided Guidance for Federal Information Security, but Missed a Reporting Deadline and Its Reporting

Guidance to Agencies Did Not Sufficiently Address a FISMA Element

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 from 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.

As of June 2019, OMB had not issued its annual FISMA report to Congress for fiscal year 2018. OMB officials stated that the lapse in appropriations during the start of 2019 caused a delay in the report's development and release. The officials declined to provide a time frame for when they expected to issue the report.

OMB Provided Numerous Guidance Documents to Agencies and Monitored Agencies' Implementation of Them

FISMA requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security. Since the start of fiscal year 2018, OMB has developed or proposed policies and generally monitored their implementation. Specifically:

- In May 2019, OMB issued policy to address federal agencies' implementation of identity, credential, and access management (ICAM).⁵⁰ Among other things, the policy requires agencies to (1) implement identity, credential, and access management guidelines,

⁵⁰Office of Management and Budget, *Enhancing Mission Delivery Through Improved Identity, Credential, and Access Management*, M-19-17 (Washington, D.C.: May 21, 2019).

standards, and directives issued by NIST, DHS, and the Office of Personnel Management; and (2) harmonize their enterprise-wide approach to ICAM governance, architecture, and acquisition through activities such as designating an integrated agency-wide ICAM governance structure and establishing solutions for ICAM services that are flexible and scalable.

- In December 2018, OMB issued a memorandum on the high-value asset (HVA)⁵¹ program⁵² that (1) outlined agency expectations for establishing agency governance; (2) required agencies to take action to improve the identification of HVAs; and (3) defined agency reporting, assessment, and remediation requirements for HVAs. In March 2018, OMB reported that agencies' continued to have challenges in mitigating security vulnerabilities identified across the federal HVA landscape in its fiscal year 2017 FISMA report to Congress. In addition, OMB required agencies to report on the implementation of security controls to protect HVAs during fiscal year 2018.
- In October 2018, OMB issued new federal information security and privacy management guidance that required agencies to (1) report on the adequacy and effectiveness of their information security programs, (2) submit a current and prioritized list of HVAs through the Homeland Security Information Network, and (3) report major incidents to DHS, OMB, Congress and their agency inspectors general.⁵³ In addition, the guidance required agencies to ensure that DHS has authorization and the information necessary to monitor and provide technical assistance related to vulnerability scanning.

⁵¹High-value assets are those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or the public confidence, civil liberties, or public health and safety of the American people. Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Assets Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

⁵²The high-value asset program established in the *Cybersecurity Strategy and Implementation Plan* (M-16-04) required all agencies to prioritize the identification and protection of high-value assets.

⁵³Office of Management and Budget, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, M-19-02 (Washington, D.C.: Oct. 25, 2018).

OMB Assessed and Reported on Agencies' Implementation of Federal Information Security Requirements, but the Number of Agencies Scheduled to Participate in CyberStat Meetings Has Declined over the Last 3 Years

In addition to developing and monitoring the implementation of information security policies, FISMA directs OMB to oversee agencies' compliance with the act's requirements to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, modification, or destruction of information or information systems. During fiscal year 2018, OMB issued four reports summarizing government-wide implementation of the information security requirements, as described below:

- In September 2018, OMB issued an assessment of intrusion detection and prevention capabilities across the federal enterprise. In its assessment, OMB briefly described federal agencies' implementation of intrusion detection and prevention capabilities through DHS's EINSTEIN sensor suite.⁵⁴
- In May 2018, OMB issued its *Federal Cybersecurity Risk Determination Report and Action Plan*.⁵⁵ For this report, OMB evaluated risk management assessment reports for 96 agencies and described actions that it and agencies plan to take to address government-wide cybersecurity gaps. Two major actions discussed in the report are: (1) federal agencies must consolidate their security operations center capabilities and processes, or migrate the security operations center as a service; and (2) OMB, DHS, and other federal agencies are to assist with implementing the cyber threat framework developed by the Office of the Director of National Intelligence.⁵⁶

⁵⁴DHS's US-CERT operates the National Cybersecurity Protection System, which is operationally known as EINSTEIN. EINSTEIN provides capabilities to detect and prevent potential cyberattacks involving the network traffic entering or exiting the networks of participating agencies.

⁵⁵Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan* (Washington, D.C.: May 2018).

⁵⁶The Office of the Director of National Intelligence developed the cybersecurity threat framework to establish a common approach to threat frameworks. According to the office, this common approach assists with establishing a shared concept, enhancing information sharing, characterizing and categorizing threat activity, and supporting common situational awareness.

- In March 2018, OMB issued its annual FISMA report to Congress for fiscal year 2017,⁵⁷ which summarized the performance of 97 agencies in implementing effective information security programs and managing risk, among other things.
- In December 2017, OMB released its *Report to the President on Federal IT Modernization*,⁵⁸ which outlined a vision and recommendations for the federal government to build a more modern and secure architecture for federal systems. For example, OMB described government-wide initiatives intended to improve the security of federal networks that emphasized perimeter network-based security protections, but had gaps in the application and data-level protections needed to provide complete security. To address these deficiencies, OMB recommended a layered defensive strategy in government-wide programs to provide greater defense-in-depth capabilities that are intended to prevent malicious actors from moving laterally across linked networks to access valuable information.

Number of Agencies Scheduled for CyberStat Meetings Significantly Declined Since Fiscal Year 2016

OMB, in coordination with DHS, is responsible for coordinating CyberStat review meetings. As mentioned previously, FISMA requires OMB to oversee agency compliance with requirements to provide information security protections on information and information systems. One means of fulfilling this oversight responsibility is through CyberStat engagements. For these engagements, OMB, in coordination with DHS, intends to engage agency leadership on Administration priorities and perform outreach to ensure that agencies are taking the appropriate actions to strengthen their cybersecurity posture.

However, since our September 2017 report on fiscal year 2016 FISMA implementation, the number of agencies that have participated in a CyberStat engagement has significantly declined.⁵⁹ In fiscal year 2016,

⁵⁷Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress Fiscal Year 2017* (Washington, D.C.: March 2018).

⁵⁸Office of Management and Budget, *Report to the President on Federal IT Modernization* (Washington, D.C.: Dec. 13, 2017).

⁵⁹GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, [GAO-17-549](#) (Washington, D.C.: Sept. 28, 2017).

OMB scheduled these engagements with 24 agencies to help develop action items that address information security risk, identify areas for targeted assistance, and track performance at the agencies throughout the year. The number of agencies scheduled to participate in an engagement decreased to five during fiscal year 2017, and decreased further to three during fiscal year 2018. As of May 2019, OMB staff in the Office of the Federal CIO informed us that the agency had not scheduled any agencies to participate in a CyberStat engagement during fiscal year 2019.

According to OMB officials in the Office of the Federal CIO, updates to the CyberStat process resulted in extended engagements between DHS, OMB, and the agencies that lasted 4 to 6 weeks or more. Beginning in fiscal year 2017, according to DHS's CyberStat concept of operations, OMB and DHS took a collaborative approach with the CyberStat process. Specifically, officials from the participating agencies, OMB's Cyber and National Security Unit, and DHS's Federal Network Resilience (FNR) division⁶⁰ collaborated through these CyberStat engagements to reach a desired performance outcome at the participating agencies.

DHS's CyberStat concept of operations states that the department focuses on agency performance in key federal information security reporting, including agency FISMA reporting, DHS reports of agency compliance with binding operational directives, and reports issued by GAO and agency inspectors general. A DHS official from the department's FNR division informed us that it uses these information security reports to make recommendations to OMB, who then decides which agencies will be scheduled to participate in a CyberStat engagement. According to OMB, the three agencies that participated in a CyberStat engagement initiated during fiscal year 2018 volunteered to do so after discussing their cybersecurity implementation issues with OMB.

However, as discussed earlier in this report, deficiencies reported in agency fiscal year 2018 FISMA reports and information security evaluation reports issued by GAO and inspectors general for fiscal year

⁶⁰The Department of Homeland Security's Federal Network Resilience division plays a vital role in providing direct cybersecurity support, coordination, and communications to all federal executive branch agencies. The division offers a broad range of cybersecurity programs and services to improve an agency's cybersecurity posture, including performance measurement and analysis, risk assessments, access to cyber-shared services, training, and technical assistance.

2018 indicate that several agencies are in need of OMB and DHS assistance to improve their information security posture. In addition, the three agencies that participated in CyberStat engagements scheduled during fiscal year 2018 saw value in changes resulting from the updated engagement process. For example, officials from the Office of the CIO (OCIO) at one of the three agencies stated that the updated process was more constructive and valuable than the prior CyberStat process that was based more on a compliance checklist. In addition, OCIO officials at all three agencies stated that the process helped improve their agencies' information security posture and that their collaboration with OMB and DHS was beneficial to assisting with FISMA implementation.

By conducting fewer CyberStat engagements with agencies, OMB loses an opportunity to assist agencies with improving their information security posture. Additionally, OMB will limit its ability to oversee specific agency efforts to provide information security protections for federal information and information systems.

Inspector General Reporting Metrics Did Not Sufficiently Cover System Security Plans

FISMA includes reporting requirements for OMB, agency CIOs and inspectors general. According to OMB's FISMA reporting guidance, OMB and DHS collaborate with interagency and inspector general partners to develop the CIO and inspector general metrics, which are intended to facilitate agencies' compliance with FISMA-related reporting requirements.⁶¹ These entities created separate sets of reporting metrics for agency CIOs and agency inspectors general.⁶²

However, the inspector general reporting metrics did not specifically address the development and maintenance of system security plans, although subordinate plans, such as system security plans, are a key element of an agency-wide information security program required by FISMA.

⁶¹Office of Management and Budget, M-19-02.

⁶²*FY 2018 CIO FISMA Metrics*, Version 2.0.1 (May 2018) and *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.0.1 (May 24, 2018).

OMB officials in the Office of the Federal CIO informed us that, while they work in coordination with CIGIE to establish the reporting metrics, CIGIE is ultimately responsible for developing the metrics. According to both the published metrics and OMB's guidance memorandum, OMB collaborates with DHS and inspector general partners to develop the IG FISMA metrics. According to representatives from CIGIE, the existence of system security plans is addressed in multiple questions within the reporting metrics, which is in alignment with OMB's focus toward ongoing assessments and authorizations.

Nevertheless, our review of the reporting metrics and supplemental evaluation guide did not identify any reference to the development and maintenance of system security plans. The lack of a defined reporting metric for addressing agency system security plans could lead to inconsistent reporting by inspectors general. Until such a metric is developed and reported on, OMB will not have reasonable assurance that inspectors general evaluations appropriately address each of the required elements of an information security program.

DHS Continued to Issue Cybersecurity-related Directives and Assist Agencies by Providing Common Security Capabilities

Under FISMA, DHS, in consultation with OMB, is responsible for carrying out various activities, including developing and overseeing the implementation of binding operational directives and providing operational and technical assistance to agencies.

Over the last 2 years, DHS had developed four binding operational directives as of April 2019, as required by FISMA. These directives instructed agencies to:

- remove and discontinue use of all present and future Kaspersky-branded⁶³ products;⁶⁴

⁶³Kaspersky-branded products include information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or any of its predecessors, successors, and parents, among others.

⁶⁴Department of Homeland Security, *Removal of Kaspersky-Branded Products*, BOD-17-01 (Washington, D.C.: Sept. 13, 2017).

- enhance email security by adopting domain-based message authentication, reporting and conformance (DMARC)⁶⁵ to prevent email spoofing and web security by ensuring all publicly accessible federal websites provides services through a secure connection;⁶⁶
- submit a current and prioritized high-value asset list to DHS and if selected, participate in risk and vulnerability assessments;⁶⁷ and
- review and remediate critical and high vulnerabilities on internet-facing systems within 15 and 30 calendar days of initial detection, respectively.⁶⁸

We have ongoing work evaluating DHS's process to develop and oversee the implementation of binding operational directives as part of another engagement. We will report on the results of this evaluation in a separate report.

DHS also provided operational and technical assistance to agencies through its Continuous Diagnostics and Mitigation (CDM) and National Cybersecurity Protection System (NCPS) programs. DHS is taking steps to deploy the CDM and NCPS capabilities to all participating federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats.

Continuous Diagnostics and Mitigation program (CDM). The program 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. In December 2018, we reported that the department was in the process of

⁶⁵DMARC is an email authentication technology that provides protection against spoofed email by ensuring that unauthenticated email messages are rejected at the mail server, even before delivery.

⁶⁶Department of Homeland Security, *Enhance Email and Web Security*, BOD-18-01 (Washington, D.C.: Oct. 16, 2017).

⁶⁷Department of Homeland Security, *Securing High Value Assets*, BOD-18-02 (Washington, D.C.: May 7, 2018).

⁶⁸Department of Homeland Security, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, BOD-19-02 (Washington, D.C.: Apr. 29, 2019).

enhancing the capabilities of federal agencies to automate network monitoring for malicious activity through its CDM program.⁶⁹

In our December report, we also recommended that DHS coordinate further with federal agencies to identify training and guidance needs for implementing CDM. DHS plans to complete implementation of our recommendation this fiscal year. In addition, we have an ongoing review to evaluate the extent to which selected agencies have effectively implemented CDM and to identify practices for effective and efficient implementation of the program. We will report on the results of this review separately.

National Cybersecurity Protection System (NCPS). The program is 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 made nine recommendations to further improve NCPS capabilities by, among other things, developing metrics that clearly measure the effectiveness of NCPS's efforts, including the quality, efficiency, and accuracy of actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information.⁷⁰ As of June 2019, DHS had implemented six of our nine recommendations and plans to implement the remainder by the end of this fiscal year.

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

⁶⁹GAO, *Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions*, [GAO-19-105](#) (Washington, D.C.: Dec. 18, 2018).

⁷⁰GAO, *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, in April 2018, NIST issued an update to its cybersecurity framework that it originally issued in February 2014. Although the cybersecurity framework was initially intended for critical infrastructure, Executive Order 13800 requires federal agencies to use the cybersecurity framework to also manage their cybersecurity risk. The revised framework includes a new section on cybersecurity measurement; an expanded explanation of using the framework for cyber supply chain risk management; refinements to authentication, authorization, and identity proofing policies within access controls; and a new section on using the cybersecurity framework to understand and assess an organization's cybersecurity risk.

In May 2017, NIST published draft guidance for agencies to use in implementing the cybersecurity framework.⁷¹ This publication is intended to provide guidance on the use of the framework in conjunction with the current and planned suite of NIST security and privacy risk management publications, such as NIST Special Publication 800-53. According to NIST officials in the agency's Computer Security Division, the agency is in the process of finalizing the implementation guidance and plans to publish the final version by the end of fiscal year 2019.

Further, in December 2018, NIST released the revised *Risk Management Framework for Information Systems and Organizations* (risk management framework).⁷² According to NIST, the update provides an integrated, robust, and flexible methodology to address security and privacy risk management. Among the changes in the updated version is the integration of privacy risk management into the existing information security risk management processes. In addition, the risk management framework includes direct references to the cybersecurity framework, which demonstrates how organizations that implement the risk

⁷¹National Institute of Standards and Technology, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies (Draft)*, IR 8170 (Gaithersburg, MD: May 2017).

⁷²National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: Dec. 20, 2018).

management framework can also achieve the outcomes of the cybersecurity framework.⁷³

In April 2019, NIST released revised guidance on vetting the security of mobile applications.⁷⁴ According to NIST, the revised publication provides guidance for planning and implementing a mobile application vetting process, developing security requirements for mobile applications, identifying appropriate tools for testing mobile applications, and determining if a mobile application is acceptable for deployment on an organization's mobile devices.

In addition, NIST is currently developing a privacy framework to help improve agencies' privacy risk management. In April 2019, NIST issued a discussion draft for its privacy framework.⁷⁵ According to the discussion draft, NIST will use feedback received on the discussion draft to develop a preliminary draft of the privacy framework, which is intended to assist organizations in identifying, assessing, and responding to privacy risks. Further, the framework is intended to foster the development of innovative approaches to protecting individuals' privacy and increase trust in systems, products and services. According to NIST officials, the agency continues to engage stakeholders, both nationally and internationally, through roundtable meetings, webinars, and public workshops to solicit stakeholder input to inform development of this framework. NIST's website states that the agency anticipates publishing the privacy framework in October 2019.

Conclusions

Federal agencies continued to have deficiencies in implementing information security programs and practices. Inspectors general reported that 18 of 24 CFO Act agencies did not have effective agency-wide information security programs in fiscal year 2018. In addition, most of the

⁷³National Institute of Standards and Technology, *Information Technology Laboratory Bulletin February 2019—The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk* (Gaithersburg, MD: February 2019).

⁷⁴National Institute of Standards and Technology, *Vetting the Security of Mobile Applications*, Special Publication 800-163, Revision 1 (Gaithersburg, MD: April 2019).

⁷⁵National Institute of Standards and Technology, *NIST Privacy Framework: An Enterprise Risk Management Tool (Discussion Draft)* (Gaithersburg, MD: Apr. 30, 2019).

selected agencies had deficiencies in the five core security functions. We and the inspectors general have made thousands of recommendations aimed at improving information security programs and practices over the years. Implementation of these recommendations will assist agencies in strengthening their information security policies and practices.

OMB, DHS, and NIST have issued directives and guidance and implemented programs that, to some extent, have improved agencies' security posture. However, OMB has not issued its report to Congress on the effectiveness of agencies' information security policies and practices for fiscal year 2018, although the report was due several months ago. Further, while agencies indicated that the collaborative CyberStat engagements with DHS and OMB have aided with their FISMA implementation, the number of these engagements has declined significantly. In addition, the OMB-approved metrics that inspectors general use to evaluate FISMA implementation do not include one of the elements—system security plans—required by FISMA for information security programs. By not including this element, oversight of agencies' information security programs has been diminished.

Recommendations for Executive Action

We are making the following three recommendations to OMB:

The Director of OMB should submit the statutorily required report to Congress on the effectiveness of agencies' information security policies and practices during the preceding year. (Recommendation 1)

The Director of OMB should expand its coordination of CyberStat review meetings for those agencies with a demonstrated need for assistance in implementing information security. (Recommendation 2)

The Director of OMB should collaborate with CIGIE to ensure that the inspector general reporting metrics include the FISMA-required information security program element for system security plans. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB and the 28 selected agencies for review and comment. In response, OMB provided comments orally

and via email in which the office, respectively, generally concurred with our first two recommendations and concurred with a revised version of our third recommendation.

Specifically, in oral comments, officials in the Office of the Federal Chief Information Officer noted actions that they said OMB plans to take to address our first two recommendations. According to these officials, the office plans to issue its fiscal year 2018 report to Congress on the effectiveness of agencies' information security policies and practices in the near future. In addition, the office plans to continue to collaborate with DHS to identify information security gaps at agencies and work with agencies to address those gaps in CyberStat meetings or by other means.

With regard to our third recommendation, the officials expressed concern with the wording of the recommendation in our draft report, which related to OMB updating the IG metrics. They noted that CIGIE, rather than OMB, is responsible for updating these metrics. Accordingly, we revised the recommendation to emphasize the need for OMB to collaborate with CIGIE.

In a subsequent email from our OMB liaison, the office concurred with the revised recommendation. The office emphasized its plans to continue working collaboratively with the inspector general community to assist with improving and evolving the metrics to ensure that the metrics address FISMA requirements.

OMB also provided technical comments, which we incorporated, as appropriate.

In addition, five of the 28 selected agencies provided written responses regarding the draft report:

- In its response (reprinted in appendix III), the Department of Housing and Urban Development stated that it had reviewed our draft report and had no comments.
- In its comments (reprinted in appendix IV), the Department of Veterans Affairs stated that it remains committed to complying with the requirements of FISMA and to safeguarding the department's systems and data, which support the delivery of care, benefits, and services to veterans. The department also stated that it continues to

prioritize efforts to address our prior information security-related recommendations to the department.

- In its response (reprinted in appendix V), the Environmental Protection Agency stated that it had reviewed our draft report and had no comments.
- In its comments (reprinted in appendix VI), the Social Security Administration stated that it will continue to improve its cybersecurity safeguards and looks forward to receiving additional guidance to assist the agency with its efforts.
- In its comments (reprinted in appendix VII), the U.S. Agency for International Development stated that it has developed, documented, and implemented an agency-wide program to provide security for its information and systems, pointing out that its inspector general reported that the agency had an effective program in fiscal year 2018. The agency also cited its commitment to continuing compliance with FISMA's requirements and to safeguarding its information technology services to facilitate its mission.

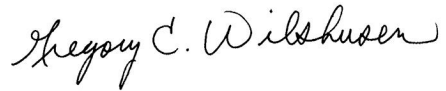
Further, four of the selected agencies—the Departments of Commerce, Homeland Security, and Transportation, as well as the National Science Foundation—also provided technical comments which we have incorporated in the report, where appropriate.

The remaining 19 selected agencies provided emails stating that they had no comments on the report. These agencies were the Departments of Agriculture, Defense, Education, Energy, Health and Human Services, the Interior, Justice, Labor, State, and the Treasury; and the Federal Communications Commission; Federal Retirement Thrift Investment Board; General Services Administration; Merit System Protection Board; National Aeronautics and Space Administration; Nuclear Regulatory Commission; Office of Personnel Management; Presidio Trust; and Small Business Administration.

We are sending copies of this report to appropriate congressional committees, the Director of OMB, the heads of the CFO Act agencies and their inspectors general, the heads of four selected non-CFO Act agencies, and other interested congressional parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen 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. GAO staff who made key contributions to this report are listed in appendix VIII.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the reported adequacy and effectiveness of selected federal agencies' information security policies and practices and (2) evaluate the extent to which the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) have implemented their government-wide *Federal Information Security Modernization Act of 2014 (FISMA)* requirements.

To describe the reported adequacy and effectiveness of federal agencies' information security policies and practices, we analyzed our, agency, and inspectors general information security-related reports for 16 selected agencies.¹ Our selection of 16 agencies included 12 *Chief Financial Officers (CFO) Act of 1990* agencies and four non-CFO Act agencies.² To select the 12 CFO Act agencies, we first ranked the 23 civilian CFO Act agencies by the number of information security systems each agency reported operating in fiscal year 2017.³ We then separated the agencies into large, medium, and small categories based on the number of systems they reported, and selected four agencies from each category using a random number generator. To select the four non-CFO Act agencies, we listed the 73 non-CFO Act agencies reported in OMB's annual FISMA report to Congress for fiscal year 2017 and then randomly

¹These reports were either issued in fiscal year 2018 or covered fiscal year 2018 (i.e., issued in fiscal year 2019).

²The 24 *Chief Financial Officers Act of 1990* 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.

³We did not include the Department of Defense in the scope of our selection because the number of systems operated by the department was not publicly reported for fiscal year 2017.

selected four agencies.⁴ Although we randomly selected agencies and assured we had CFO Act and non-CFO Act agencies, due to the small number of agencies examined, results based on these agencies do not generalize beyond the agencies reviewed.

The 16 agencies were the Departments of the Agriculture, Commerce, Education, Housing and Urban Development, Justice, Labor, State, and the Treasury; the Environmental Protection Agency; Federal Communications Commission; Federal Retirement Thrift Investment Board; Merit Systems Protection Board; National Aeronautics and Space Administration; Presidio Trust; Small Business Administration; and the Social Security Administration. For these agencies, we analyzed, categorized, and summarized weaknesses identified in inspector general and GAO reports using the NIST *Framework for Improving Critical Infrastructure Cybersecurity*⁵ (cybersecurity framework) core security functions and the eight elements of information security programs required by FISMA.

In addition, for the 24 agencies covered by the CFO Act, we summarized (1) the inspector general ratings of agency-wide information security programs and (2) the inspector general designation of information security as a significant deficiency or a material weakness for financial reporting systems as reported for fiscal year 2018. For the 23 civilian agencies covered by the CFO Act, we summarized fiscal year 2018 agency Chief Information Officer (CIO) reports of their agency's progress in meeting targets for implementing cyber capabilities supporting the Administration's cybersecurity-related Cross-Agency Priority (CAP) goal.⁶

To gain insight into how agencies collect, report, and ensure the accuracy and completeness of the FISMA data they report, we analyzed documentation describing and supporting the processes at eight of the 16 selected agencies to ensure the accuracy and completeness of those data. We also interviewed officials at the eight agencies to obtain additional information on the quality controls implemented on the system

⁴Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report to Congress Fiscal Year 2017* (Washington, D.C.: March 2018).

⁵National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: April 16, 2018).

⁶We did not include the Department of Defense in the scope of this summary because the department did not publicly report this information for fiscal year 2018.

used for FISMA reporting. The eight agencies selected were the Departments of Education, Justice, Labor, and the Treasury; the Federal Communications Commission; National Aeronautics and Space Administration; Presidio Trust; and the Small Business Administration. These agencies were randomly selected from the list of 16 agencies described above. Based on our assessment, we determined that the data were sufficiently reliable for the purpose of our reporting objectives.

To evaluate the extent to which OMB, DHS, and NIST have implemented FISMA requirements, we analyzed the FISMA provisions to identify federal responsibilities for OMB, DHS, and NIST. We evaluated documentation of these agencies' government-wide responsibilities to determine if the agencies were meeting FISMA requirements, including documentation obtained from their websites. Specifically, for OMB, we collected and reviewed information security-related policies and guidance that it issued since we last reported in September 2017. We also obtained reports issued by OMB to determine the extent to which the agency had overseen the policies and guidelines it issued, as well as other agency efforts for improving information security. In addition, we analyzed fiscal year 2018 inspector general and CIO FISMA reporting metrics to determine if the metrics sufficiently addressed the agency-wide information security program elements required by FISMA. We also interviewed OMB officials to obtain information on any actions they have planned or taken to improve the information security posture of the federal government.

Further, we interviewed OMB and DHS officials to understand their process for scheduling CyberStat engagements with senior agency officials. We also interviewed officials at the three agencies that participated in a CyberStat engagement initiated during fiscal year 2018 to understand the benefits and challenges of their collaboration with OMB and DHS.

For DHS, we reviewed and summarized a recently issued GAO report describing updates to the department's Continuous Diagnostic and Mitigation Program and National Cybersecurity Protection System.⁷ We also collected and summarized the binding operational directives issued by DHS over the last 2 years. Further, we interviewed DHS officials to

⁷GAO, *Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions*, [GAO-19-105](#) (Washington, D.C.: Dec. 18, 2018)

obtain information on any actions they have planned or taken to improve the information security posture of the federal government.

For NIST, we collected and summarized the standards and guidance issued or updated by the agency since the start of fiscal year 2018. We also interviewed NIST officials and obtained information on draft standards and guidance to describe NIST's current and planned efforts to help improve the information security posture of the federal government.

We conducted this performance audit from December 2018 to July 2019 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.

Appendix II: Cybersecurity Framework

The National Institute of Standards and Technology established the cybersecurity framework to provide guidance for cybersecurity activities within the private sector and government agencies at all levels.¹ The cybersecurity framework consists of five core functions: identify, protect, detect, respond, and recover. Within the five functions are 23 categories and 108 subcategories that define discrete outcomes for each function, as described in table 5.

Table 5: National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity

	Identify (ID) core function
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.
	ID.AM-2: Software platforms and applications within the organization are inventoried.
	ID.AM-3: Organizational communication and data flows are mapped.
	ID.AM-4: External information systems are catalogued.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions	ID.BE-1: The organization’s role in the supply chain is identified and communicated.
	ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk,	ID.GV-1: Organizational cybersecurity policy is established and communicated.
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.

¹National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

Identify (ID) core function

environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

ID.GV-4: Governance and risk management processes address cybersecurity risks.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1: Asset vulnerabilities are identified and documented.

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.

ID.RA-3: Threats, both internal and external, are identified and documented.

ID.RA-4: Potential business impacts and likelihoods are identified.

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

ID.RA-6: Risk responses are identified and prioritized.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

ID.RM-2: Organizational risk tolerance is determined and clearly expressed.

ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.

Protect (PR) core function

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

PR.AC-2: Physical access to assets is managed and protected.

PR.AC-3: Remote access is managed.

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

Protect (PR) core function	
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained.
	PR.AT-2: Privileged users understand their roles and responsibilities.
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
	PR.AT-4: Senior executives understand their roles and responsibilities.
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected.
	PR.DS-2: Data-in-transit is protected.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.
	PR.DS-4: Adequate capacity to ensure availability is maintained.
	PR.DS-5: Protections against data leaks are implemented.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
	PR.DS-7: The development and testing environment(s) are separate from the production environment.
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.
	PR.IP-3: Configuration change control processes are in place.
	PR.IP-4: Backups of information are conducted, maintained, and tested.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
	PR.IP-6: Data is destroyed according to policy.
	PR.IP-7: Protection processes are improved.
	PR.IP-8: Effectiveness of protection technologies is shared.
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	PR.IP-10: Response and recovery plans are tested.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
	PR.IP-12: A vulnerability management plan is developed and implemented.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Protect (PR) core function

system components are performed consistent with policies and procedures.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
	PR.PT-2: Removable media is protected and its use restricted according to policy.
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
	PR.PT-4: Communications and control networks are protected.
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Detect (DE) core function

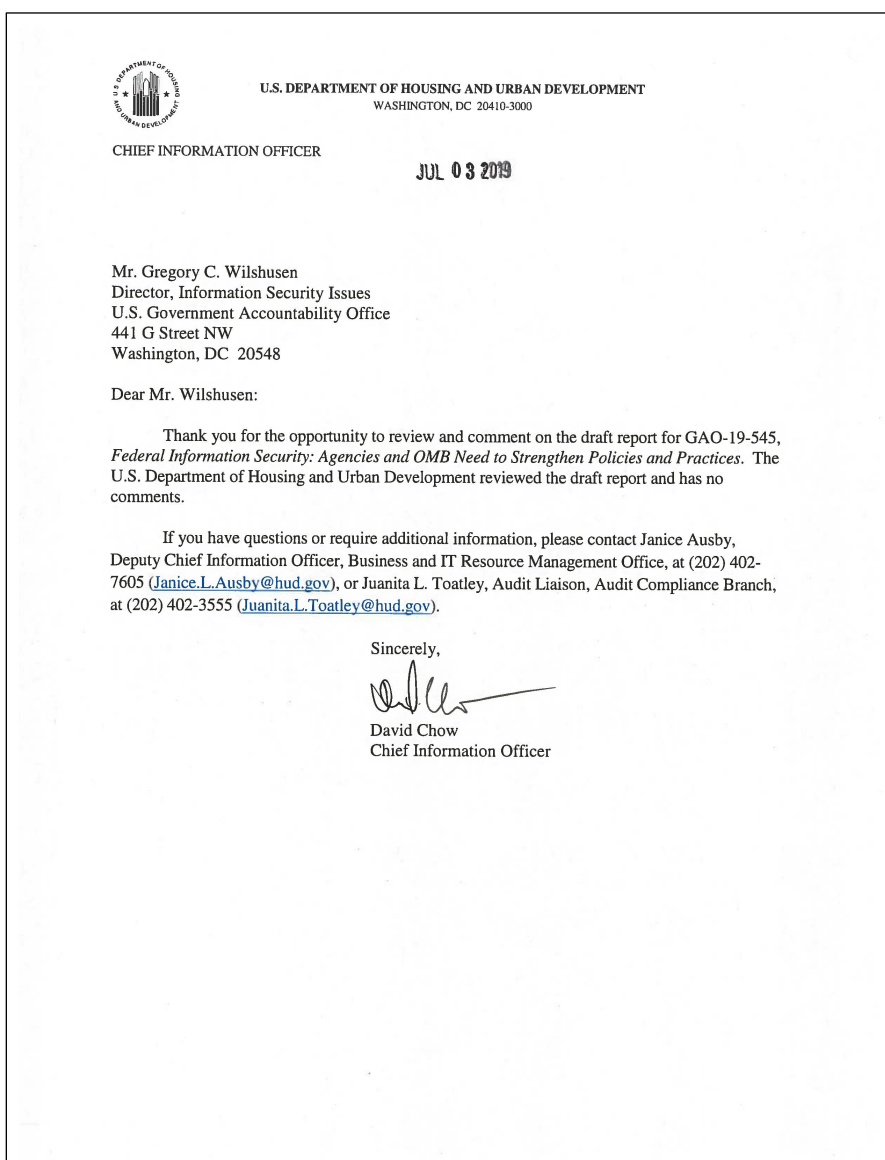
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
	DE.AE-4: Impact of events is determined.
	DE.AE-5: Incident alert thresholds are established.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
	DE.CM-4: Malicious code is detected.
	DE.CM-5: Unauthorized mobile code is detected.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
	DE.CM-8: Vulnerability scans are performed.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.
	DE.DP-2: Detection activities comply with all applicable requirements.
	DE.DP-3: Detection processes are tested.
	DE.DP-4: Event detection information is communicated.
	DE.DP-5: Detection processes are continuously improved.

Respond (RS) core function	
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed.
	RS.CO-2: Incidents are reported consistent with established criteria.
	RS.CO-3: Information is shared consistent with response plans.
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.
	RS.AN-2: The impact of the incident is understood.
	RS.AN-3: Forensics are performed.
	RS.AN-4: Incidents are categorized consistent with response plans.
	RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained.
	RS.MI-2: Incidents are mitigated.
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned.
	RS.IM-2: Response strategies are updated.

Recover (RC) core function	
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.
	RC.IM-2: Recovery strategies are updated.
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, internet service providers, owners of attacking systems, victims, other computer security incident response teams, and vendors).	RC.CO-1: Public relations are managed.
	RC.CO-2: Reputation is repaired after an incident.
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

Source: National Institute of Standards and Technology. | GAO-19-545

Appendix III: Comments from the Department of Housing and Urban Development



**Appendix III: Comments from the Department
of Housing and Urban Development**

2

cc:

Kevin R. Cooke, Jr., Principal Deputy Chief Information Officer, Q
Janice (Ausby) Boyd, Deputy CIO for Business and IT Resource Management, QRM
Tracy K. Bigesby, Deputy Chief Information Security Officer, OCIO, QS
Wynee Watts-Mitchell, Director, Audit Compliance Branch, OCIO, QMAC
Juanita Toatley, IT Specialist, Audit Compliance Branch, OCIO, QMAC
Helen McBride, Senior Advisor to the Principal Deputy Chief Information Officer, Q
Michael A. Simms, Administrative Officer, Administrative Services Branch, OCIO, QMAS
Steven J. Parker, Jr., Management Analyst, Administrative Services Branch, OCIO, QMAS
Oscar V. Franklin, Director, Audit Liaison Division, OCFO, FMA

Text of Appendix III: Comments from the Department of Housing and Urban Development

Page 1

Mr. Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office 441 G Street NW

Washington, DC 20548 Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the draft report for GAO-19-545,

Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices. The

U.S. Department of Housing and Urban Development reviewed the draft report and has no comments.

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,

David Chow

Chief Information Officer

Page 2

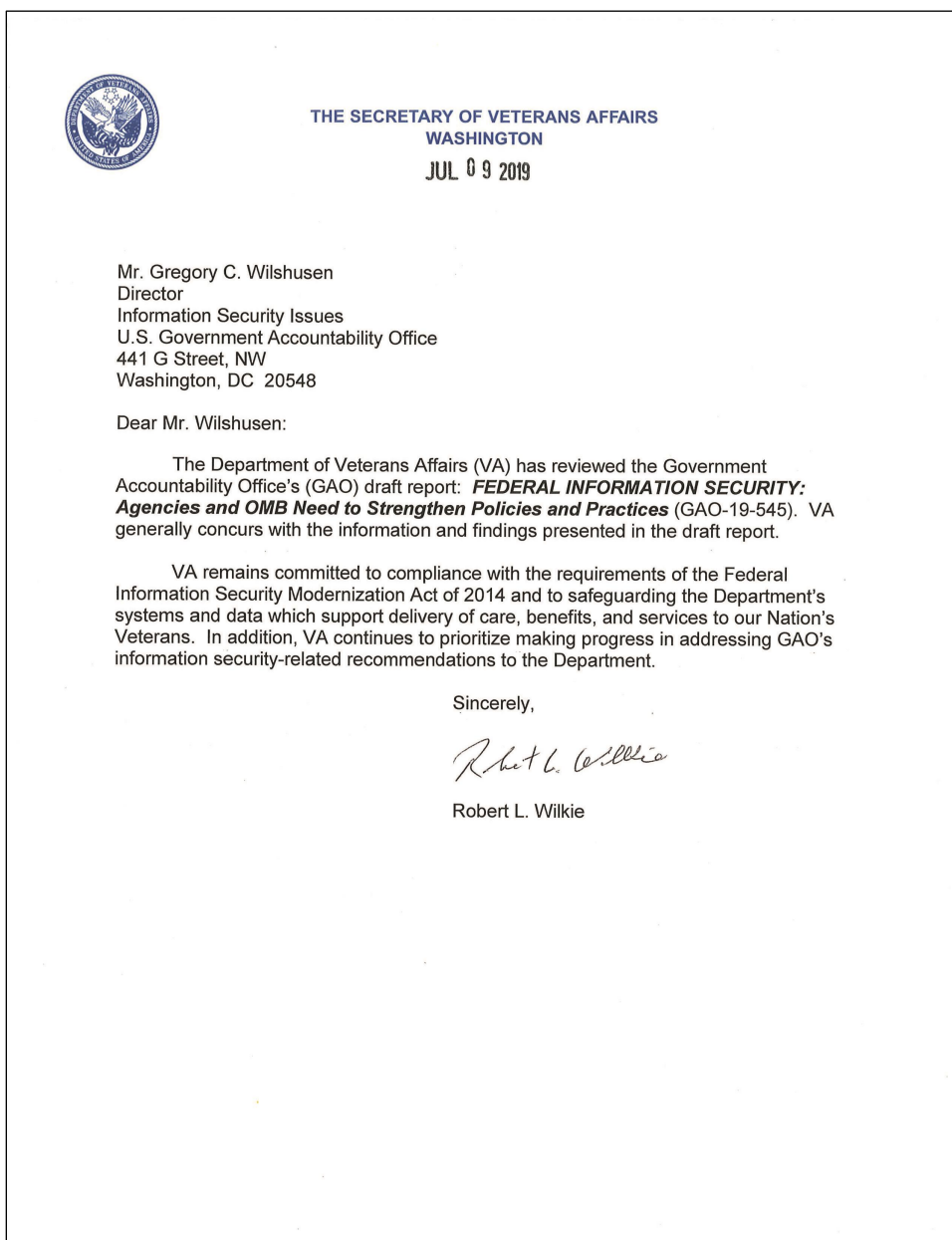
cc: Patricia Randolph Williams , OMS Janice Jablonski, OMS

Robert McKinney, OISP Jeff Anouilh, OISP

Lee Kelly, OISP Torina Anderson, OISP Annette Morant, OCFO Jeffrey L Knott,
GAO

Di'Mond N. Spencer, GAO Andrew Ahn, GAO

Appendix IV: Comments from the Department of Veterans Affairs



Text of Appendix IV: Comments from the Department of Veterans Affairs

Mr. Gregory C. Wilshusen Director

Information Security Issues

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

Washington, DC 20548 Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government

Accountability Office's (GAO) draft report: FEDERAL INFORMATION SECURITY:
Agencies and OMB Need to Strengthen Policies and Practices (GAO-19-545). VA
generally concurs with the information and findings presented in the draft report.

VA remains committed to compliance with the requirements of the Federal
Information Security Modernization Act of 2014 and to safeguarding the
Department's systems and data which support delivery of care, benefits, and
services to our Nation's Veterans. In addition, VA continues to prioritize making
progress in addressing GAO's information security-related recommendations to the
Department.

Sincerely,

Robert L. Wilkie

Appendix V: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JUL 08 2019

OFFICE OF MISSION SUPPORT

Mr. Gregory C. Wilshusen,
Director, Information Security Issues
U.S. Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Draft Report, GAO-19-545, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices* (103151).

The purpose of this letter is to provide the Environmental Protection Agency's (EPA's) response to the report.

GAO had no recommendations for the EPA, however, there are several tables and figures where EPA is included in GAO's aggregate analysis.

EPA reviewed the Draft Report and has no corrections or additional comments.

If you require additional information or would like to discuss further, please contact Patricia Randolph Williams at (202) 564-0204.

Sincerely,

A handwritten signature in black ink, appearing to read "Vaughn Noga".

Vaughn Noga
Chief Information Officer and
Deputy Assistant Administrator for Environmental
Information

**Appendix V: Comments from the
Environmental Protection Agency**

cc: Patricia Randolph Williams, OMS
Janice Jablonski, OMS
Robert McKinney, OISP
Jeff Anouilh, OISP
Lee Kelly, OISP
Torina Anderson, OISP
Annette Morant, OCFO
Jeffrey L Knott, GAO
Di'Mond N. Spencer, GAO
Andrew Ahn, GAO

Text of Appendix V: Comments from the Environmental Protection Agency

Page 1

Mr. Gregory C. Wilshusen,

Director, Information Security Issues

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

Washington , DC 20548 Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Draft Report, GAO-19-545, Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices (I-103151).

The purpose of this letter is to provide the Environmental Protection Agency's (EPA's) response to the report.

GAO had no recommendations for the EPA, however, there are several tables and figures where EPA is included in GAO's aggregate analysis.

EPA reviewed the Draft Report and has no corrections or additional comments.

If you require additional information or would like to discuss further, please contact Patricia Randolph Williams at (202) 564-0204.

Since rely ,

Vaughn Noga

Chief Information Officer and

Deputy Assistant Administrator for Environmental Information

Appendix VI: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

July 9, 2019

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "FEDERAL INFORMATION SECURITY: Agencies and OMB Need to Strengthen Policies and Practices" (GAO-19-545). We will continue to improve our cybersecurity safeguards, and we look forward to receiving additional guidance to assist us with these efforts.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

A handwritten signature in blue ink that reads "Stephanie Hall".

Stephanie Hall
Acting, Deputy Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Text of Appendix VI: Comments from the Social Security Administration

July 9, 2019

Mr. Gregory C. Wilshusen

Director, Information Security Issues

United States Government Accountability Office 441 G Street, NW

Washington, DC 20548 Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "FEDERAL INFORMATION SECURITY: Agencies and OMB Need to Strengthen Policies and Practices" (GAO-19-545). We will continue to improve our cybersecurity safeguards, and we look forward to receiving additional guidance to assist us with these efforts.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Acting, Deputy Chief of Staff

Appendix VII: Comments from the U.S. Agency for International Development



Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices (GAO-19-545)

Dear Mr. Wilshusen:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices* (GAO-19-545).

USAID is committed to supporting improvements to our information-security program, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The GAO acknowledges this commitment in the draft report by recognizing that our Agency is among the six of 24 civilian Department and Agencies covered by the Chief Financial Officers Act whose Inspectors General reported they had an effective Institution-wide information-security program in Fiscal Year 2018.

In compliance with the FISMA, USAID has developed, documented, and implemented an Agency-wide program to provide security for the information and information systems that support our operations and assets. USAID is committed to continuing compliance with the FISMA's requirements and to safeguarding our information technology services to facilitate our mission.

I am transmitting this letter for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

A handwritten signature in blue ink, which appears to read 'Frederick M. Nutt', is positioned above the typed name.

Frederick M. Nutt
Assistant Administrator
Bureau for Management

Text of Appendix VII: Comments from the U.S. Agency for International Development

Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office 441 G Street, N.W.

Washington, D.C. 20226

Re: Federal Information Security: Agencies and OMB Need to Strengthen Policies
and Practices (GAO-19-545)

Dear Mr. Wilshusen:

I am pleased to provide the formal response of the U.S. Agency for International
Development (USAID) to the draft report produced by the U.S. Government
Accountability Office (GAO) titled, Federal Information Security: Agencies and OMB
Need to Strengthen Policies and Practices (GAO-19-545).

USAID is committed to supporting improvements to our information-security
program, as required by the Federal Information Security Modernization Act of 2014
(FISMA).

The GAO acknowledges this commitment in the draft report by recognizing that our
Agency is among the six of 24 civilian Department and Agencies covered by the
Chief Financial Officers Act whose Inspectors General responded they had an
effective Institution-wide information security program in Fiscal Year 2018.

In compliance with the FISMA, USAID has developed, documented, and
implemented an Agency-wide program to provide security for the information and
information systems that support our operations and assets. USAID is committed to
continuing compliance with the FISMA's requirements and to safeguarding our
information technology services to facilitate our mission.

I am transmitting this letter for inclusion in the GAO's final report. Thank you for the
opportunity to respond to the draft report, and for the courtesies extended by your
staff while conducting this engagement.

Sincerely,

Frederick M. Nutt Assistant Administrator Bureau for Management

Appendix VIII: GAO Contacts and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (assistant director), Di'Mond Spencer (analyst-in-charge), Andrew Ahn, Chris Businsky, Fatima Jahan, and Priscilla Smith made key contributions to this report.

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 (<https://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 <https://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, <https://www.gao.gov/ordering.htm>.

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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



Please Print on Recycled Paper.