United States Government Accountability Office

Report to Congressional Committees

December 2018

INFORMATION SECURITY

Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions

Accessible Version

GAO-19-105

GAO
Highlights

Highlights of GAO-19-105, a report to congressional committees

December 2018

INFORMATION SECURITY

Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions

Why GAO Did This Study

Federal agencies are dependent on information systems to carry out operations. The risks to these systems are increasing as security threats evolve and become more sophisticated. To reduce the risk of a successful cyberattack, agencies can deploy intrusion detection and prevention capabilities on their networks and systems.

GAO first designated federal information security as a government-wide high-risk area in 1997. In 2015, GAO expanded this area to include protecting the privacy of personally identifiable information. Most recently, in September 2018, GAO updated the area to identify 10 critical actions that the federal government and other entities need to take to address major cybersecurity challenges.

The federal approach and strategy for securing information systems is grounded in the provisions of the *Federal Information Security Modernization Act of 2014* and Executive Order 13800. The act requires agencies to develop, document, and implement an agency-wide program to secure their information systems. The Executive Order, issued in May 2017, directs agencies to use the National Institute of Standards and Technology's cybersecurity framework to manage cybersecurity risks.

The *Federal Cybersecurity Enhancement Act of 2015* contained a provision for GAO to report on the effectiveness of the government's approach and strategy for securing its systems. GAO determined (1) the reported effectiveness of agencies'

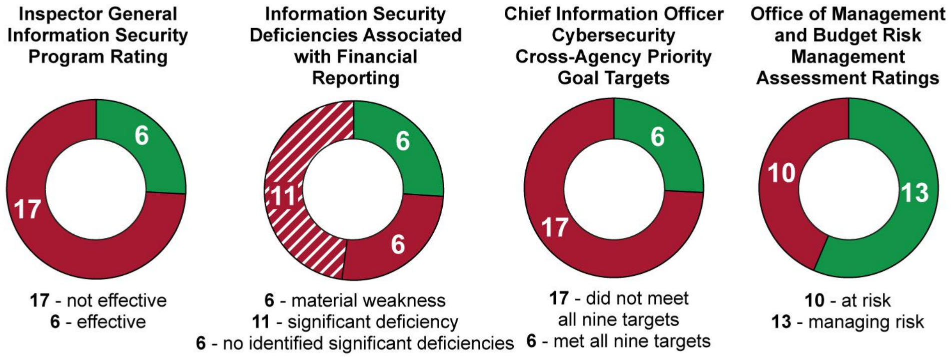
View GAO-19-105. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act) have often not effectively implemented the federal government's approach and strategy for securing information systems (see figure below). Until agencies more effectively implement the government's approach and strategy, federal systems will remain at risk. To illustrate:

- As required by Office of Management and Budget (OMB), inspectors general (IGs) evaluated the maturity of their agencies' information security programs using performance measures associated with the five core security functions—identify, protect, detect, respond, and recover. The IGs at 17 of the 23 agencies reported that their agencies' programs were not effectively implemented.
- IGs also evaluated information security controls as part of the annual audit of their agencies' financial statements, identifying material weaknesses or significant deficiencies in internal controls for financial reporting at 17 of the 23 civilian CFO Act agencies.
- Chief information officers (CIOs) for 17 of the 23 agencies reported not meeting all elements of the government's cybersecurity cross-agency priority goal. The goal was intended to improve cybersecurity performance through, among other things, maintaining ongoing awareness of information security, vulnerabilities, and threats; and implementing technologies and processes that reduce malware risk.
- Executive Order 13800 directed OMB, in coordination with the Department of Homeland Security (DHS), to assess and report on the sufficiency and appropriateness of federal agencies' processes for managing cybersecurity risks. Using performance measures for each of the five core security functions, OMB determined that 13 of the 23 agencies were managing overall enterprise risks, while the other 10 agencies were at risk. In assessing agency risk by core security function, OMB identified a few agencies to be at high risk (see figure at the top of next page).

Fiscal Year 2017 Indicators of the 23 Selected Civilian Agencies' Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems



Inspector General Information Security Program Rating
17 - not effective
6 - effective

Information Security Deficiencies Associated with Financial Reporting
6 - material weakness
11 - significant deficiency
6 - no identified significant deficiencies

Chief Information Officer Cybersecurity Cross-Agency Priority Goal Targets
17 - did not meet all nine targets
6 - met all nine targets

Office of Management and Budget Risk Management Assessment Ratings
10 - at risk
13 - managing risk

Source: GAO analysis of agency fiscal year 2017 *Federal Information Security Modernization Act of 2014* and agency financial reports for fiscal year 2017. | GAO-19-105

Why GAO Did This Study (cont.)

implementation of the government's approach and strategy; (2) the extent to which DHS and OMB have taken steps to facilitate the use of intrusion detection and prevention capabilities to secure federal systems; and (3) the extent to which agencies reported implementing capabilities to detect and prevent intrusions.

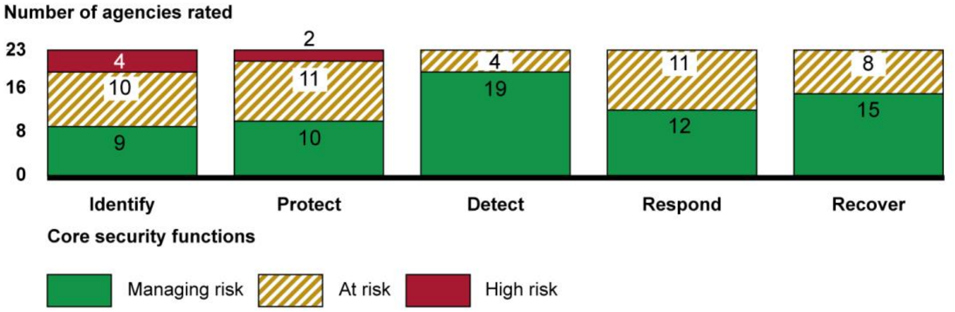
To address these objectives, GAO analyzed OMB reports related to agencies' information security practices including OMB's annual report to Congress for fiscal year 2017. GAO also analyzed and summarized agency-reported security performance metrics and IG-reported information for the 23 civilian CFO Act agencies. In addition, GAO evaluated plans, reports, and other documents related to DHS intrusion detection and prevention programs, and interviewed OMB, DHS, and agency officials.

What GAO Recommends

GAO is making two recommendations to DHS, to among other things, coordinate with agencies to identify additional needs for training and guidance. GAO is also making seven recommendations to OMB to, among other things, direct the Federal CIO to update the mandated report with required information, such as detecting advanced persistent threats. DHS concurred with GAO's recommendations. OMB did not indicate whether it concurred with the recommendations or not.

What GAO Found (cont.)

Risk Management Assessment Ratings by Core Security Function for the 23 Civilian *Chief Financial Officers Act of 1990* Agencies, Fiscal Year 2017



Source: GAO analysis of Office of Management and Budget Fiscal Year 2017 *Federal Information Security Modernization Act of 2014 Annual Report To Congress.* | GAO-19-105

DHS and OMB facilitated the use of intrusion detection and prevention capabilities to secure federal agency systems, but further efforts remain. For example, in response to prior GAO recommendations, DHS had improved the capabilities of the National Cybersecurity Protection System (NCPS), which is intended to detect and prevent malicious traffic from entering agencies' computer networks. However, the system still had limitations, such as not having the capability to scan encrypted traffic. The department was also in the process of enhancing the capabilities of federal agencies to automate network monitoring for malicious activity through its Continuous Diagnostics and Mitigation (CDM) program. However, the program was running behind schedule and officials at most agencies indicated the need for additional training and guidance. Further, the Federal CIO issued a mandated report assessing agencies' intrusion detection and prevention capabilities, but the report did not address required information, such as the capability of NCPS to detect advanced persistent threats, and a cost/benefit comparison of capabilities to commercial technologies and tools.

Selected agencies had not consistently implemented capabilities to detect and prevent intrusions into their computer networks. Specifically, the agencies told GAO that they had not fully implemented required actions for protecting email, cloud services, host-based systems, and network traffic from malicious activity. For example, 21 of 23 agencies had not, as of September 2018, sufficiently enhanced email protection through implementation of DHS' directive on enhanced email security. In addition, less than half of the agencies that use cloud services reported monitoring these services. Further, most of the selected 23 agencies had not fully implemented the tools and services available through the first two phases of DHS's CDM program. Until agencies more thoroughly implement capabilities to detect and prevent intrusions, federal systems and the information they process will be vulnerable to malicious threats.

Contents

Tables

Figures

Abbreviations

BOD	binding operational directive
CAP	cross-agency priority
CDM	continuous diagnostics and mitigation
CFO	chief financial officer

CIO	chief information officer
CSIP	*Cybersecurity Strategy and Implementation Plan*
DEFEND	Dynamic and Evolving Federal Enterprise Network Defense
DHS	Department of Homeland Security
DNS	domain name system
FISMA	*Federal Information Security Modernization Act*
IG	inspectors general
IPv6	Internet protocol version 6
NCPS	National Cybersecurity Protection System
NSD	network security deployment
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SCADA	supervisory control and data acquisition
SIEM	security information and event management
SP	special publication
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

December 18, 2018

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

The Honorable Michael McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Federal agencies are dependent on computerized (cyber) information 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. Further, many of these systems contain vast amounts of personally identifiable information,[1] thus, making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents when they occur.

The risks to information systems supporting the federal government are increasing as security threats continue to evolve and become more sophisticated. These risks include escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

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

Compounding these risks, computer networks and systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. These systems 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 attack surface.

Our previous reports, and those by federal inspectors general, describe persistent information security weaknesses that place federal agencies at risk of disruption or inappropriate disclosure of sensitive information. Accordingly, GAO made more than 3,000 recommendations to agencies since 2010 aimed at addressing cybersecurity shortcomings. Although many of these recommendations have been addressed, approximately 700 had not been implemented as of November 2018.

The federal approach and strategy for securing information systems is grounded in the provisions of the *Federal Information Security Modernization Act of 2014* (FISMA)[2] and Executive Order 13800.[3] FISMA requires agencies to develop, document, and implement an agency-wide information security program to secure federal information systems, and assigns oversight responsibilities to the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB). The executive order establishes a policy for managing cybersecurity risk and directs agencies to use the National Institute of Standards and Technology (NIST) cybersecurity framework[4] to manage these risks.

[2] The *Federal Information Security Modernization Act of 2014* (FISMA 2014), enacted as Pub. L. No. 113-283, 128 Stat. 3073 (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 both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[3] The 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).

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

GAO first designated federal information security as a government-wide high-risk area almost 22 years ago in 1997.[5] In 2003,[6] we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015,[7] we further expanded this area to include protecting the privacy of personally identifiable information. We continued to identify federal information security as a government-wide high-risk area in our February 2017 high-risk update report.[8]

Most recently, in September 2018,[9] we provided an update to the information security high-risk area by identifying four major cybersecurity challenges facing the nation and 10 critical actions that the federal government and other entities needed to take to address them. These actions included developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace. In this update, we noted that establishing a comprehensive cybersecurity strategy and performing effective oversight were a major challenge.

The *Federal Cybersecurity Enhancement Act of 2015*,[10] which was enacted December 18, 2015, included a provision for GAO to report on the effectiveness of the federal government's approach and strategy for securing agency information systems, including intrusion detection and prevention capabilities.[11] Our specific objectives were to assess: (1) the reported effectiveness of selected agencies' implementation of the federal government's approach and strategy to securing agency information systems; (2) the extent to which OMB and DHS have facilitated the use of intrusion detection and prevention capabilities to secure federal agency

[5] GAO, *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).

[6] GAO, *High Risk Series: An Update,* GAO-03-119 (Washington, D.C.: January 2003).

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

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

[9] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622, (Washington, D.C.: Sep. 6, 2018).

[10] The act is a part of the *Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, div. N, title II, subtitle B, 129 Stat. 2242, 2963-2975 (Dec. 18, 2015).

[11] According to NIST, intrusions are defined as attempts to bypass the security mechanisms of a computer or network or to compromise the confidentiality, integrity and availability of the information they contain.

information systems; and (3) the extent to which selected agencies reported implementing capabilities to detect and prevent intrusions.

To address the first objective, we reviewed annual reports from OMB and the 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act).[12] These reports were related to the implementation of FISMA for fiscal year 2017, which was the most recent fiscal year for which the reports were available. In addition, we examined performance metrics related to the cybersecurity cross-agency priority (CAP) goal[13] for fiscal years 2016 and 2017 for the 23 agencies. We also reviewed the financial statement audit reports for the 23 civilian agencies for fiscal years 2016 and 2017. Because we focused our work on the 23 civilian agencies, results from these reviews are not generalizable to the entire federal government.

For the second objective, we collected and reviewed information security-related documents from OMB and DHS and compared them to requirements of the *Federal Cybersecurity Enhancement Act of 2015*. We also interviewed knowledgeable officials from OMB and DHS regarding their agencies' efforts to fulfill requirements of the act.

In addition, we assessed the extent to which DHS had improved the capabilities of the National Cybersecurity Protection System (NCPS).[14] To do this, we assessed the department's actions to implement nine recommendations GAO previously made to, among other things, enhance

[12] The 23 civilian *Chief Financial Officers Act of 1990* agencies are the Departments of 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. We did not include the Department of Defense in the scope of our audit because the *Federal Cybersecurity Enhancement Act of 2015* only applies to civilian agencies.

[13] The cybersecurity CAP goal was established by the prior administration as part of implementing the requirement in the *GPRA Modernization Act of 2010*, Pub. L. No. 111-352, § 5, 124 Stat. 3866, 3873 (Jan. 4, 2011) codified at 31 U.S.C. § 1120(a)(1)(B).

[14] NCPS, designed and operated by DHS, was developed to be one of the tools to aid federal agencies in mitigating information security threats. The system is to provide DHS with the capability to provide four cyber-related services to federal agencies: intrusion detection, intrusion prevention, analytics, and information sharing.

the system and better define requirements for future capabilities.[15] We also reviewed documents and interviewed DHS officials to determine other actions, beyond those related to our recommendations, that the department had taken to improve the system. Further, we held semi-structured interviews[16] with knowledgeable officials from the 23 civilian CFO Act agencies to obtain their views on the intrusion detection and prevention capabilities made available by DHS. The results of these interviews are not generalizable to all federal agencies.

To address the third objective, we summarized information from our semi-structured interviews about reported capabilities implemented at the 23 civilian CFO Act agencies to detect and prevent intrusions. We also analyzed security status reports from DHS. See appendix I for additional details on our objectives, scope, and methodology.

We conducted this performance audit from December 2017 to December 2018 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

Cybersecurity incidents continue to impact federal entities and the information they maintain. According to OMB's 2018 annual FISMA report to Congress, agencies reported 35,277 information security incidents to DHS's U.S. Computer Emergency Readiness Team (US-CERT)[17] in fiscal year 2017. As shown in figure 1, these incidents involved threat vectors,

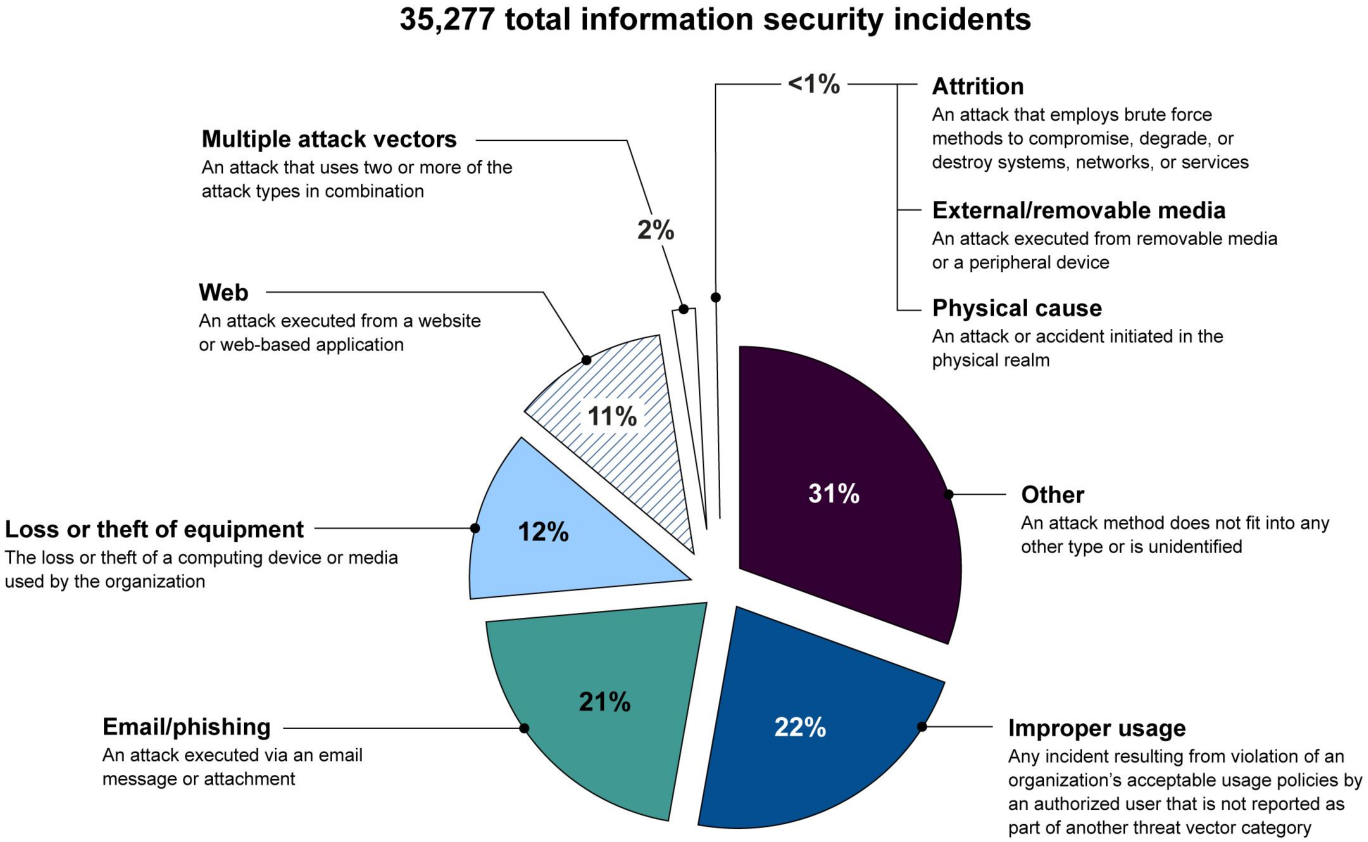
[15] GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System,* GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

[16] A semi-structured interview methodology generally involves asking a similar subset of questions of multiple interviewees. We used a semi-structured interview format with both closed- and open-ended questions. The intent of our open-ended questions was to engage the agency officials in a conversation about the topics being discussed.

[17] Within DHS, US-CERT is a component of the National Cybersecurity and Communications Integration Center. It serves as the central federal information security incident center specified by FISMA.

such as web-based attacks, phishing attacks,[18] and the loss or theft of computer equipment, among others.[19]

Figure 1: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2017



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2017. | GAO-19-105

[18] Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

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

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

- In 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 5 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.
- In June 2015, the Office of Personnel Management reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had compromised its systems and the files related to background investigations for at least 21.5 million individuals.

Federal Law and Policy Prescribe the Federal Approach and Strategy for Securing Information Systems

The federal approach and strategy for securing information systems is prescribed by federal law and policy. FISMA sets requirements for effectively securing federal systems and information. In addition, the *Federal Cybersecurity Enhancement Act of 2015* requires protecting federal networks through the use of federal intrusion prevention and detection capabilities. Further, Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[20] directs agencies to manage cybersecurity risks to the federal enterprise by,

[20] The 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).

among other things, using the NIST *Framework for Improving Critical Infrastructure Cybersecurity*[21] (cybersecurity framework).

The *Federal Information Security Modernization Act of 2014* Sets Requirements for Securing Federal Systems and Information

FISMA was enacted to improve federal cybersecurity and clarify government-wide responsibilities. The law is intended to provide for improved oversight of federal agencies' information security programs. Specifically, the law provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The law is also intended to ensure the effective oversight of information security risks, including those throughout civilian, national security, and law enforcement agencies.

FISMA assigns OMB and DHS oversight roles in ensuring federal agencies' compliance with the law. 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. The law further requires DHS to administer the implementation of agency information security policies and practices for non-national security information systems, in consultation with OMB, by developing, issuing, and overseeing implementation of binding operational directives;[22] monitoring agency implementation of information security policies and practices; and convening meetings with senior agency officials to help ensure their effective implementation of information security policies and practices, among other things.

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

[22] Binding operational directives are compulsory directions to agencies in order to safeguard federal information and information systems, are in accordance with OMB guidelines, and may be revised or repealed by the OMB Director. FISMA authorizes DHS to develop and issue binding operational directives to federal agencies and oversee their implementation by agencies. DHS has developed and issued seven binding operational directives, instructing agencies to, among other things, enhance e-mail security by removing certain insecure protocols.

FISMA assigned to NIST the responsibility for developing standards and guidelines that include minimum information security requirements. To this end, NIST has issued several publications to provide guidance for agencies in implementing an information security program. For example, NIST Special Publication (SP) 800-53[23] provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.

FISMA also assigns to the head of each executive branch agency, responsibility for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. The law also delegates to the agency chief information officer (CIO), or comparable official, the authority to ensure compliance with FISMA requirements. The CIO is responsible for designating a senior agency information security officer whose primary duty is information security.

In addition, the law requires agencies to develop, document, and implement an agency-wide information security program to secure federal information systems. Specifically, 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. Further, FISMA requires agencies to comply with DHS binding operational directives, OMB policies and procedures, and NIST federal information processing standards.

FISMA also has reporting requirements for OMB and federal agencies. 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 of the United States on the adequacy and effectiveness of their information security policies, procedures, and practices, as well as their compliance with FISMA.

[23] National 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).

The *Federal Cybersecurity Enhancement Act of 2015* Articulates Requirements for Protecting Federal Networks through the Use of Federal Intrusion Prevention and Detection Capabilities

The *Federal Cybersecurity Enhancement Act of 2015*, among other things, sets forth authority for enhancing federal intrusion prevention and detection capabilities among federal entities. The act contains several provisions for DHS and OMB. Specifically, the act requires that DHS deploy, operate, and maintain capabilities to prevent and detect cybersecurity risks in network traffic traveling to or from an agency's information system. DHS is to make these capabilities available for use by any agency.

In addition, the act requires DHS to improve intrusion detection and prevention capabilities, as appropriate, by regularly deploying new technologies and modifying existing technologies. The act also requires OMB and DHS, in consultation with appropriate agencies, to review and update government-wide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks, and to brief appropriate congressional committees.

The Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Directs Agencies to Use the Cybersecurity Framework for Managing Risks

In May 2017, the President signed Executive Order 13800, which sets policy for managing cybersecurity risk as an executive branch enterprise. Specifically, it outlines actions to enhance cybersecurity across federal agencies and critical infrastructure to improve the nation's cyber posture and capabilities against cybersecurity threats. 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 agency to use the NIST cybersecurity framework to manage those risks.

The cybersecurity framework, which provides guidance for cybersecurity activities, is based on five core security functions:

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **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.[24]
- **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 are 23 categories and 108 subcategories that include controls for achieving the intent of each function.[25] Appendix II provides a description of the cybersecurity framework categories and subcategories of controls.

GAO Has Reported on Challenges Related to Establishing a Comprehensive Cybersecurity Strategy

In February 2013, we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government, as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector. However, we noted that no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[26] Accordingly, we recommended that the White House

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

[25] For 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, including NIST Special Publication 800-53.

[26] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented,* GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

Cybersecurity Coordinator[27] in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy.[28] These characteristics would include, among other things, milestones and performance measures for major activities to address stated priorities; cost and resources needed to accomplish stated priorities; and specific roles and responsibilities of federal organizations related to the strategy's stated priorities.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. For example, in September 2018,[29] we reported that recent executive branch initiatives that identify cybersecurity priorities for the federal government provide a good foundation toward establishing a more comprehensive strategy. Nevertheless, we pointed out that additional efforts were needed to address all of the desirable characteristics of a national strategy that we recommended.

Specifically, recently issued executive branch strategy documents[30] did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. For example, these strategy documents did not generally include:

- milestones and performance measures to gauge results;
- resources needed to carry out the goals and objectives; and

[27] In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Cyberspace Policy Review, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation's digital infrastructure.

[28] In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. See GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[29] GAO-18-622.

[30] These initiatives include Executive Order 13800, the National Security Strategy, and DHS Cybersecurity Strategy.

- clearly defined roles and responsibilities for key agencies, such as DHS, the Department of Defense, and OMB.

Ultimately, we determined that a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

Subsequent to our September 2018 report, the President issued the *National Cyber Strategy* on September 20, 2018.[31] The strategy builds upon Executive Order 13800 and describes actions that federal agencies and the administration are to take to, among other things, secure federal information systems. For example, the strategy states that the administration is expected to further enable DHS to secure federal department and agency networks, to include ensuring that DHS has appropriate access to agency information systems for cybersecurity purposes and can take and direct action to safeguard systems. In addition, the strategy states that the administration plans to continue with its existing efforts underway to transition agencies to shared services and infrastructure and that DHS is to have appropriate visibility into those services and infrastructure to improve cybersecurity posture.[32]

DHS Offers Federal Agencies Capabilities Intended to Detect and Prevent Intrusions to Federal Information Systems

DHS's Network Security Deployment (NSD) division manages cybersecurity programs that are intended to improve the cybersecurity posture of the federal government. Among these programs, NCPS provides a capability to detect and prevent potentially malicious network traffic from entering agencies' networks. In addition, the Continuous Diagnostics and Mitigation (CDM) program provides tools to agencies intended to identify and resolve cyber vulnerabilities on an ongoing basis.

[31] The White House, *National Cyber Strategy* (Washington, D.C.: Sept. 20, 2018).

[32] Evaluating the *National Cyber Strategy* to determine if it included the key elements of desirable characteristics discussed in GAO-18-622 was not within the scope of this review.

DHS's National Cybersecurity Protection System Is Intended to Detect and Prevent Cyber Intrusions

Operated by DHS's US-CERT, NCPS is intended to detect and prevent cyber intrusions into agency networks, analyze network data for trends and anomalous data, and share information with agencies on cyber threats and incidents. Deployed in stages, this system, operationally known as EINSTEIN, has provided increasing capabilities to detect and prevent potential cyberattacks involving the network traffic entering or exiting the networks of participating federal agencies. Table 1 provides an overview of the EINSTEIN deployment stages to date.

Table 1: Overview of the National Cybersecurity Protection System (NCPS) Deployment, 2003-2013

Operational name	Deployment year	NCPS objective	Description
EINSTEIN 1	2003	Intrusion detection	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections.[a]
EINSTEIN 2	2009	Intrusion detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts DHS's U.S. Computer Emergency Readiness Team (US-CERT) when specific network activity matching the predetermined signatures is detected.[b]
EINSTEIN 3 Accelerated	2013	Intrusion detection Intrusion prevention	Automatically blocks malicious traffic from entering or leaving federal civilian agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision making using DHS-developed indicators of malicious cyber activity to develop signatures.[c]

Source: GAO analysis of Department of Homeland Security (DHS) data. | GAO-19-105

[a] The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[b] Signatures are recognizable, distinguishing patterns associated with cyberattacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

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

In January 2016, we reported the projected total life-cycle cost of the program was approximately $5.7 billion through fiscal year 2018.[33] In addition, according to the Federal CIO, Congress appropriated $468 million in fiscal year 2017 and $402 million in fiscal year 2018 for NCPS.

In that report, we also noted that NCPS was partially, but not fully, meeting most of its stated system objectives.[34] Although the system's intrusion detection capabilities provided the ability to detect known patterns of malicious activity on agency networks, it was limited in its capabilities to identify potential threats using anomaly-based detection. We also reported that although DHS had developed metrics for measuring the performance of NCPS, the metrics did not gauge the

[33] GAO-16-294.

[34] GAO-16-294.

quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities.

The department had also identified needs for future capabilities, but had not defined requirements for the capability to detect threats entering and exiting cloud service providers. Further, DHS had not considered specific vulnerability information for agency information systems in making risk-based decisions about future intrusion prevention capabilities.

Accordingly, we made nine recommendations to DHS to, among other things, enhance the NCPS capabilities for meeting its objectives and better define requirements for future capabilities. DHS agreed with each of our nine recommendations and indicated that it would take steps to address them.

DHS's Continuous Diagnostics and Mitigation Program Provides Agencies with Tools and Services Intended to Secure Agency Systems

DHS's CDM program provides federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that, at an agency level, is intended to alert network managers and enable the agency to allocate resources based on the risk. Summary data from each participating agency's dashboard is expected to be transmitted to the Federal Dashboard where the data can be used to inform decisions about cybersecurity risks across the federal government.

There are four phases of CDM implementation:

- **Phase 1**—involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. According to the *Cybersecurity Strategy and Implementation Plan*,[35] DHS purchased phase 1 tools

[35] Office of Management and Budget, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, Memorandum M-16-04 (Washington, D.C.: Oct. 30, 2015). CSIP identified objectives, key actions, responsibilities, and timeframes for completing actions that were intended to strengthen cybersecurity at federal civilian agencies.

and integration services for all participating agencies in fiscal year 2015. DHS plans to have all phase 1 tools deployed at participating agencies by the end of the second quarter of fiscal year 2019.

- **Phase 2**—intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. According to the *Cybersecurity Strategy and Implementation Plan*, DHS was to provide agencies with additional phase 2 capabilities throughout fiscal year 2016, with the full suite of CDM phase 2 capabilities delivered by the end of that fiscal year. However, according to the OMB FISMA *Annual Report to Congress for Fiscal Year 2017*, the CDM program began deploying Phase 2 tools and sensors during fiscal year 2017.[36] DHS plans to have all phase 2 tools deployed at participating agencies by the end of fiscal year 2019.
- **Phase 3**—includes detection capabilities that are intended to assess agency network activity and identify any anomalies that may indicate a cybersecurity compromise.[37] Full operating capability[38] for phases 1, 2, and 3 is planned to be achieved by the end of fiscal year 2022.[39]
- **Phase 4**—intends to provide tools to (1) protect data at rest, in transit, and in use; (2) prevent loss of data; and (3) manage and mitigate data breaches. According to CDM program officials, phase 4 has not been approved and no tools have been selected.

NIST Recommends That Federal Agencies Deploy Intrusion Detection and Prevention Capabilities

An approach for protecting systems against cybersecurity compromise is for federal agencies to build successive layers of defense mechanisms at

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

[37] CDM phase 3 also includes, among other things, completing remaining required phase 1 activities and integrating all deployed phase 2 tools into agency and federal dashboards.

[38] DHS's NSD division considers an agency to have reached full operating capability for a given CDM phase when the full set of capabilities for the phase has been fully deployed across the agency (i.e., the capabilities have been installed, configured, integrated, and data is feeding into the agency's dashboard).

[39] According to CDM program officials, initial operational capability—a project milestone attained when the capabilities for a phase have been fully deployed to at least five agencies—for phase 3 is planned by the end of fourth quarter fiscal year 2019.

strategic points in their information technology infrastructures. This approach, commonly referred to as defense in depth, entails implementing a series of protective mechanisms so that if one mechanism fails to detect and prevent an attack, another will provide a backup defense. By utilizing defense in depth, federal agencies can reduce the risk of a successful cyberattack by implementing intrusion detection and prevention capabilities.

NIST has developed guidelines for protecting agency information systems using intrusion detection and prevention capabilities. For example, NIST SP 800-53 recommends that agencies strategically deploy capabilities and perform monitoring of their systems to include observation of events occurring on their network and at the external boundary of their network. In addition, NIST SP 800-94 provides agencies with guidance in designing, implementing, configuring, securing, monitoring, and maintaining such capabilities.[40]

As part of their defense-in-depth approach and, as recommended by the NIST guidelines, agencies can deploy the following list of capabilities, among others, on their networks to detect and prevent an attack:

- **Protecting email from intrusions:** According to OMB,[41] email, by way of phishing attacks, remains one of the most common threat vectors across the government. Methods for protecting email include encryption, false email alerts, and anti-spear-phishing training.[42]
- **Monitoring cloud services:** Cloud vendors provide services to agencies, including Software as a Service,[43] Platform as a Service,[44]

[40] National Institute of Standards and Technology, *Guide to Intrusion Detection and Prevention Systems*, Special Publication 800-94 (Gaithersburg, MD: February 2007).

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

[42] Spear phishing represents a digital form of social engineering that uses authentic looking emails, websites, or instant messages that are closely tailored to their intended audience to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.

[43] In Software as a Service, the agency uses the service provider’s applications, which are accessible from various client devices through an interface such as a web browser (e.g., web-based e-mail system). The agency does not manage or control the underlying infrastructure or the individual application capabilities.

and Infrastructure as a Service.[45] As agencies increasingly rely on cloud services, monitoring traffic to and from their cloud service providers helps to ensure that agencies detect malicious traffic.

- **Using host-based intrusion prevention:** Host-based intrusion prevention systems provide defense at an individual system or device level by protecting against malicious activities. Host-based capabilities include memory-based protection[46] and application whitelisting.[47]
- **Monitoring external and internal traffic:** Agencies can monitor external and internal traffic, including: encrypted traffic, traffic between workstations and servers on the network, and direct connections to outside entities such as universities. Monitoring traffic helps to ensure that agencies detect malicious activity.
- **Using security information and event management:** A security information and event management capability produces real-time alerts and notifications of significant security events. Security alerts and notifications can provide the agency with better situational awareness regarding possible intrusion activity.

Selected Agencies Were Not Effectively Implementing the Federal Government's Approach and Strategy to Securing Information Systems

According to inspectors general, agency CIOs, and OMB reports on federal information security practices, many agencies were not effectively

[44] In Platform as a Service, the agency deploys its own or acquired applications created using programming languages and tools supported by the provider. The agency does not manage or control the underlying infrastructure, but controls and configures the deployed applications.

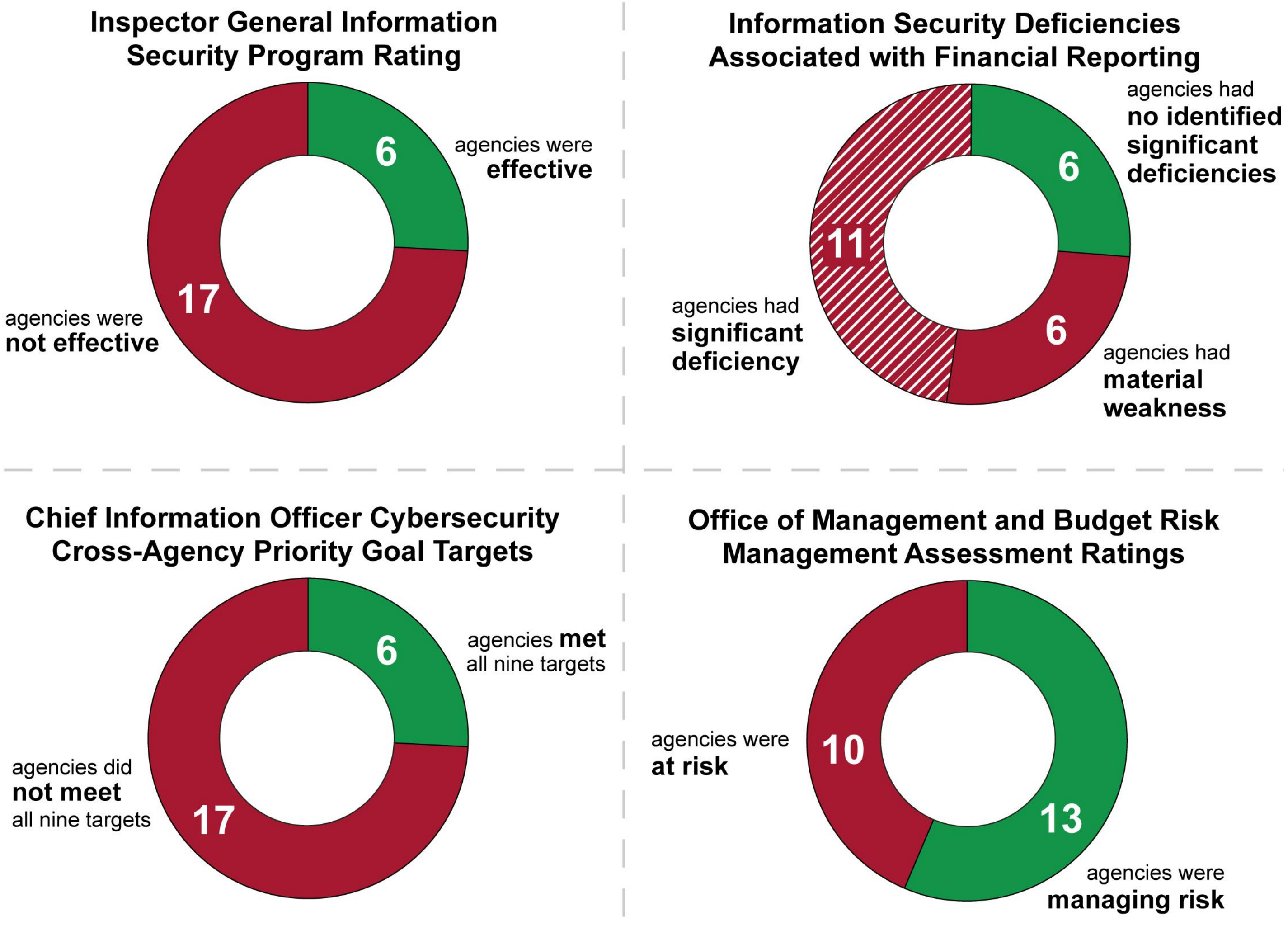
[45] In Infrastructure as a Service, the agency has the capability to provision processing, storage, networks, and other fundamental computing resources and run its own software, including operating systems and applications. The agency does not manage or control the underlying infrastructure but controls and configures operating systems, storage, deployed applications, and possibly, selected networking components (e.g., host firewalls).

[46] Memory based protections are safeguards that protect memory from unauthorized code execution.

[47] An application whitelist is a list of applications and application components that an agency has authorized for use on its hosts.

implementing the federal government's approach and strategy to securing information systems as of fiscal year 2017. Agencies' inspectors general determined that most of the 23 civilian CFO Act agencies did not have effective agency-wide information security programs. They also reported that agencies did not have effective information security controls in place, leading to deficiencies in internal control over financial reporting. In addition, the CIOs demonstrated that, during fiscal years 2016 and 2017, most agencies had not met all targets for the cybersecurity CAP goal for improving cybersecurity performance. Further, based on FISMA metrics reported for fiscal year 2017, OMB determined that 13 of the 23 agencies were managing risks to their enterprise, while the other 10 agencies were at risk of ineffectively identifying, protecting, detecting, responding to, and if necessary, recovering from cyber intrusions. Figure 2 summarizes agencies' efforts to implement the government's approach and strategy for securing information systems as of fiscal year 2017.

Figure 2: Fiscal Year 2017 Indicators of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies' Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems



Source: GAO analysis of agency fiscal year 2017 *Federal Information Security Modernization Act of 2014* and agency financial reports for fiscal year 2017. | GAO-19-105

Appendix III includes a table that provides an additional overview of the effectiveness of each agency's implementation of the government's approach and strategy to securing information systems.

Inspectors General Determined That Most Selected Agencies Did Not Have Effective Information Security Programs or Controls in Place as of Fiscal Year 2017

Inspectors general determined that more than half of the 23 civilian CFO Act agencies did not have effective agency-wide information security programs as of fiscal year 2017. Further, in agency financial statement audit reports for fiscal year 2017, inspectors general reported that, despite improvements being made in information security practices, most of the civilian CFO Act agencies continued to exhibit deficiencies in information security controls. As a result of these deficiencies, inspectors general reported material weaknesses or significant deficiencies in internal control over financial reporting.

Inspectors General Indicate That Few Agencies Had Effective Information Security Programs

FISMA requires inspectors general to determine the effectiveness of their respective agencies' information security programs. To do so, FISMA reporting instructions[48] direct 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.

The ratings used to evaluate the effectiveness of agencies' information security programs are based on a five-level maturity model, as described in table 2.

[48] Inspectors general FISMA metrics and reporting instructions were developed as a collaborative effort amongst OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal CIO Council. The FISMA metrics and reporting instructions provide reporting requirements across key areas to be addressed in the independent assessment of agencies information security programs. See *Fiscal Year 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (April 17, 2017).

Table 2: Inspector General Reporting Metrics Maturity Model

Maturity level	Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess those policies procedures, and strategy, and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: GAO analysis of Fiscal Year 2017 Inspector General *Federal Information Security Modernization Act of 2014* Reporting Metrics, April 17, 2017. | GAO-19-105

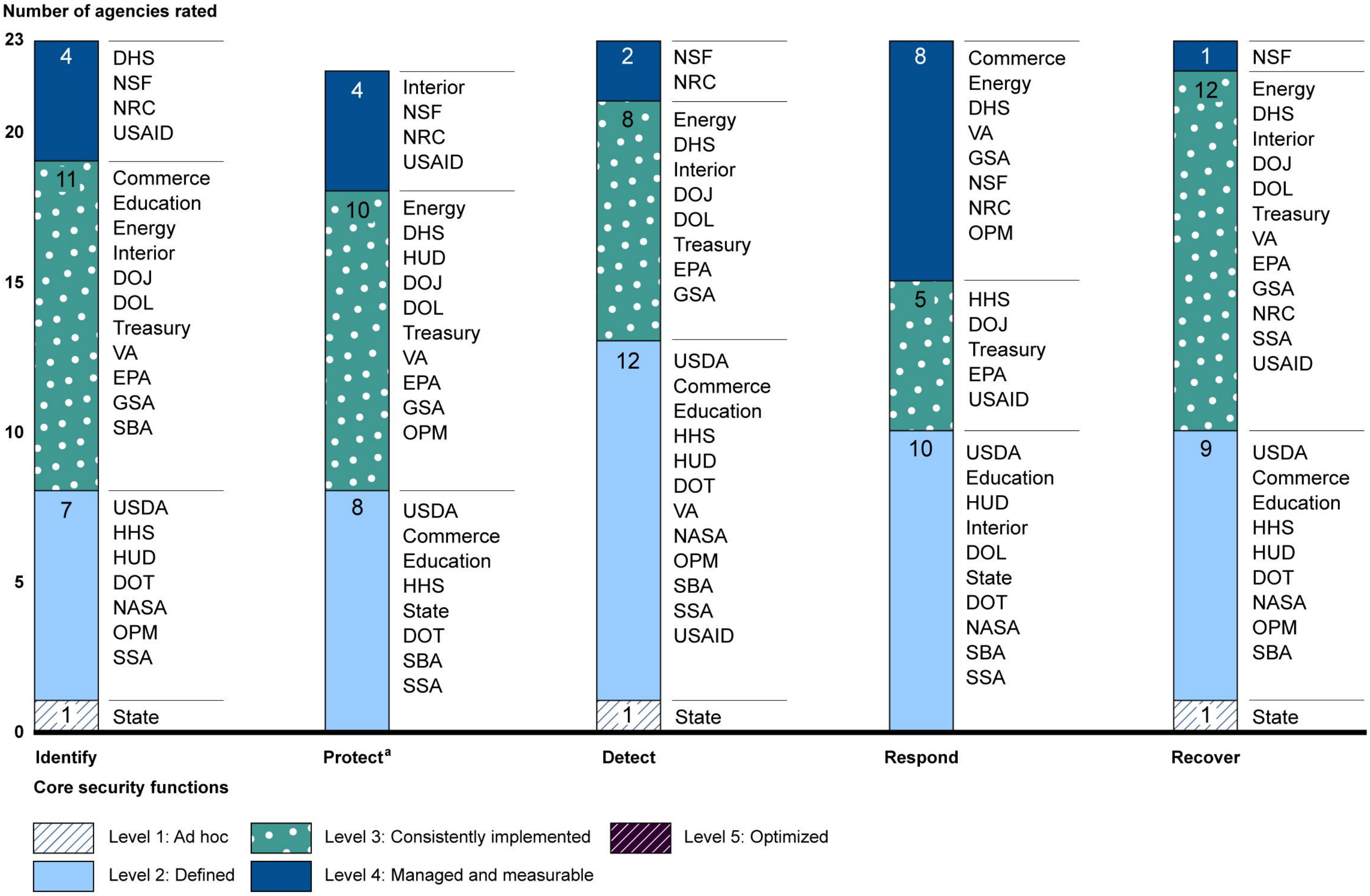
According to this maturity model, Level 4 (managed and measurable) represents an effective level of security.[49] Therefore, if an inspector general rates the agency's information security program at Level 4 or Level 5, then that agency is considered to have an effective information security program.[50]

For fiscal year 2017, the inspectors general for 6 of the 23 civilian CFO Act agencies reported that their agencies had an effective agency-wide information security program. More specifically, for the 5 core security functions, most inspectors general reported that their agency was at Level 3 (consistently implemented) for the *identify*, *protect*, and *recover* functions, and at Level 2 (defined) for the *detect* and *respond* functions, as shown in figure 3.

[49] NIST 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.

[50] *Fiscal Year 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (April 17, 2017).

Figure 3: Inspector General Ratings of Agencies' Information Security Policies, Procedures, and Practices Related to the Five Core Security Functions, as of Fiscal Year 2017



DHS (Department of Homeland Security), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), USAID (United States Agency for International Development), Commerce (Department of Commerce), Education (Department of Education), Energy (Department of Energy), Interior (Department of the Interior), DOJ (Department of Justice), DOL (Department of Labor), Treasury (Department of the Treasury), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), GSA (General Services Administration), SBA (Small Business Administration), USDA (United States Department of Agriculture), HHS (Department of Health & Human Services), HUD (Department of Housing and Urban Development), DOT (Department of Transportation), NASA (National Aeronautics and Space Administration), OPM (Office of Personnel Management), SSA (Social Security Administration), State (Department of State)

Source: GAO analysis of agency fiscal year 2017 *Federal Information Security Modernization Act of 2014* reports. | GAO-19-105

[a] Only 22 agencies are listed because the NASA inspector general did not provide a rating for the Protect function.

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

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)—access controls, configuration management, segregation of duties, contingency planning, and security management.[51] The reports also identify the inspectors general's designation of information security as a significant deficiency[52] or material weakness in internal control over financial reporting systems.[53]

For fiscal year 2017, inspectors general continued to identify information security control deficiencies in each of the five major control categories across the 23 civilian CFO Act agencies. The number of agencies with deficiencies in the access control and contingency planning information

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

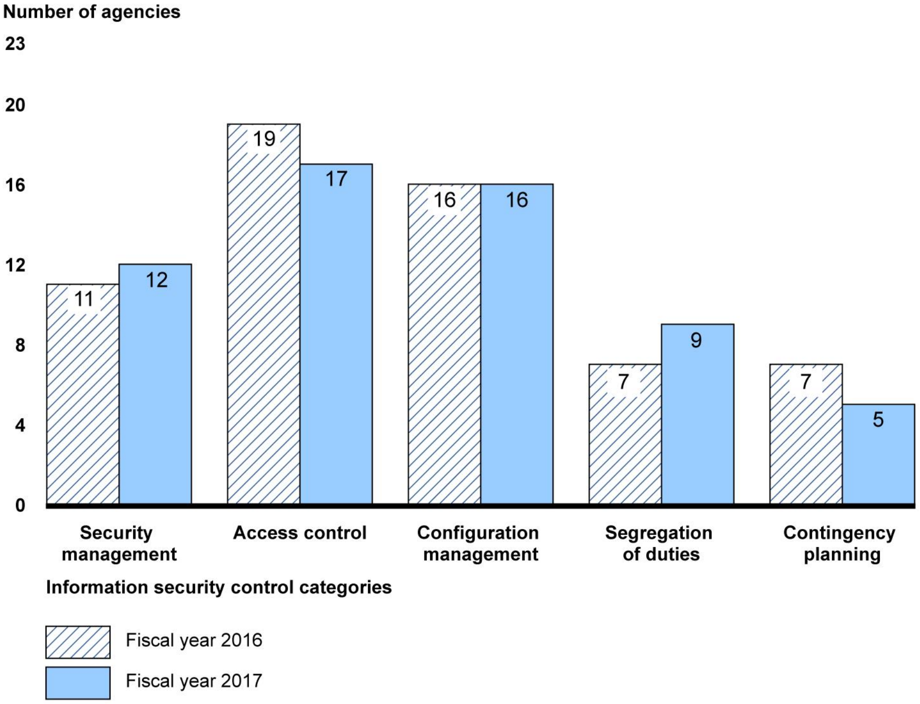
[52] A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design 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, misstatements on a timely basis.

[53] A 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.

security control categories decreased between fiscal years 2016 and 2017, according to the inspectors general.

Nevertheless, the inspectors general reported that agencies continued to exhibit deficiencies in these two control categories. In addition, the number of agencies with deficiencies in the security management and segregation of duties control categories increased from the prior year. The number of agencies reported as having deficiencies in the configuration management control category remained the same. Figure 4 shows the number of agencies that reported deficiencies in each of the information security control categories for fiscal years 2016 and 2017.

Figure 4: Number of Civilian *Chief Financial Officers Act of 1990* Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Years 2016 and 2017



Source: GAO analysis of agency financial reports for fiscal years 2016 and 2017. | GAO-19-105

Overall, inspectors general for the 23 civilian CFO Act agencies reported progress in agencies' information security practices for fiscal year 2017. Specifically, during that time, 17 inspectors general designated information security as either a significant deficiency (11) or material weakness (6) in internal control over financial reporting systems for their agencies. This is a decrease from the previous fiscal year when 19 inspectors general designated information security as a significant deficiency (12) or material weakness (7).

Most Agencies Reported Not Meeting All Targets for the Cybersecurity Cross-Agency Priority Goal in Fiscal Years 2016 and 2017

Reporting instructions contained in the fiscal year 2017 FISMA metrics[54] directed CIOs to assess their agencies’ progress toward achieving outcomes that strengthen federal cybersecurity. To do this, CIOs evaluated their agencies’ performance in reaching targets for specific FISMA reporting metrics. According to the reporting instructions, certain metrics were selected to represent the administration’s cybersecurity CAP goal. These selected metrics allowed CIOs to evaluate their agencies progress in meeting targets for that goal.

The cybersecurity CAP goal for fiscal years 2015 through 2017[55] was to improve cybersecurity performance by having an ongoing awareness of information security, vulnerabilities, and threats impacting the operating information environment; ensuring that only authorized users have access to resources and information; and implementing technologies and processes that reduce the risk of malware. The cybersecurity CAP goal consisted of three priority areas with a total of nine performance indicators. Each of the nine performance indicators had an expected level of performance, or target, for implementation. Table 3 shows the three priority areas and related performance indicators and targets of the cybersecurity CAP goal for fiscal years 2015 through 2017.

[54] Each year, OMB and DHS work with an interagency group to develop the CIO FISMA metrics. These metrics are organized around the five cybersecurity framework core security functions and track agencies’ progress in implementing cybersecurity capabilities.

[55] Although the CAP goal was in place for fiscal years 2015 through 2017, the scope of our review was for fiscal years 2016 and 2017.

Table 3: Priority Areas, Performance Indicators, and Targets for the Cybersecurity Cross-Agency Priority Goal, Fiscal Years 2015–2017

Priority area	Performance indicator	Target
Information security continuous monitoring is the provision that covers ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.	Hardware asset management	Implemented at 95 percent for the agency
Information security continuous monitoring is the provision that covers ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.	Software asset management	Implemented at 95 percent for the agency
Information security continuous monitoring is the provision that covers ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.	Vulnerability management	Implemented at 95 percent for the agency
Information security continuous monitoring is the provision that covers ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.	Secure configuration management	Implemented at 95 percent for the agency
Identity, credential, and access management is the implementation of a set of capabilities that are intended to ensure users must authenticate their identities in order to use information technology resources and have access to only those resources that are required for their job function.	Implementation of personal identity verification for unprivileged users	Implemented at 85 percent for unprivileged users
Identity, credential, and access management is the implementation of a set of capabilities that are intended to ensure users must authenticate their identities in order to use information technology resources and have access to only those resources that are required for their job function.	Implementation of personal identity verification for privileged users	Implemented at 100 percent for privileged users
Anti-phishing and malware defense is the implementation of technologies, processes, and training that are intended to reduce the risk of malware introduced through email and malicious or compromised web sites.	Anti-phishing defense	Implemented at 90 percent for 5 of the top 7 anti-phishing defenses
Anti-phishing and malware defense is the implementation of technologies, processes, and training that are intended to reduce the risk of malware introduced through email and malicious or compromised web sites.	Malware defenses	Implemented at 90 percent for 3 of the top 5 malware defenses

Priority area	Performance indicator	Target
Anti-phishing and malware defense is the implementation of technologies, processes, and training that are intended to reduce the risk of malware introduced through email and malicious or compromised web sites.	Other defenses	Implemented at 90 percent for 2 of the top 4 other defenses

Source: GAO analysis of Office of Management and Budget *Fiscal Year 2017 Federal Information Security Modernization Act of 2014 Annual Report to Congress*. | GAO-19-105

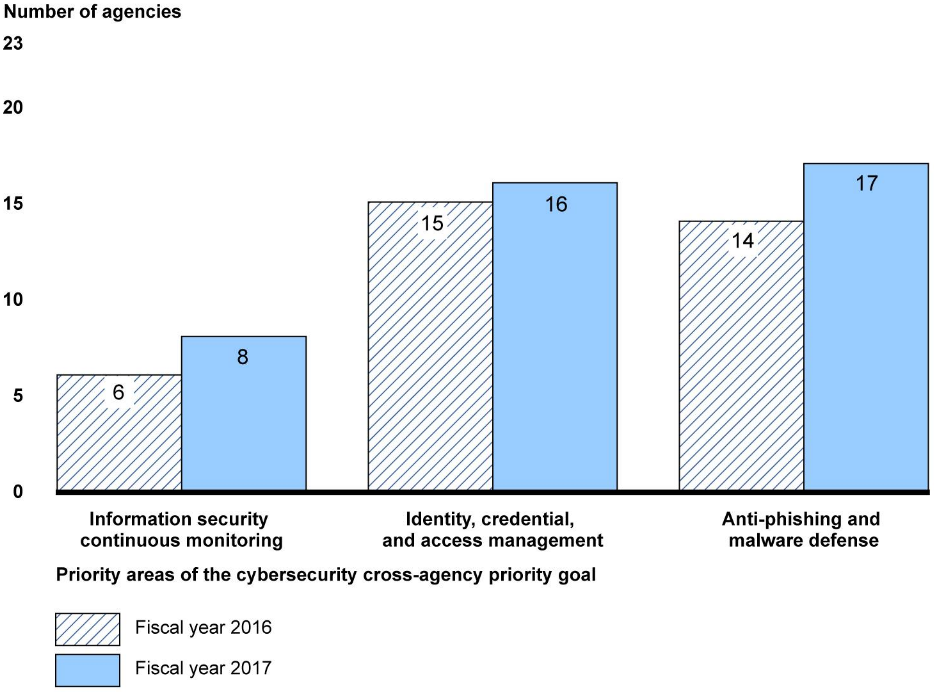
According to agency CIO assessments for fiscal year 2017, 6 of the 23 agencies met all 9 targets for the cybersecurity CAP goal. More specifically,

- 8 agencies met all four targets for the information security continuous monitoring priority area;
- 16 agencies met the two targets for the identity, credential, and access management priority area; and
- 17 agencies met all three targets for the anti-phishing and malware defense priority area.

In addition, CIOs reported that agencies were making progress in meeting the targets for the nine performance indicators for fiscal years 2016 and 2017, with increases in the number of agencies meeting the targets within each of the three priority areas.

However, although the number of agencies that met the targets in individual priority areas showed a net increase, not all agencies maintained their status. For example, the CIO for one agency reported meeting all three targets for the anti-phishing and malware defense priority area in fiscal year 2016, but reported that the agency only met two of the three targets in fiscal year 2017. Figure 5 shows the number of agencies that reported meeting each of the targets within the individual cybersecurity CAP goal priority areas for fiscal years 2016 and 2017.

Figure 5: Number of the 23 Selected Civilian Agencies That Reported Meeting Targets for the Cybersecurity Cross-Agency Priority Goal Priority Areas, Fiscal Years 2016 and 2017



Source: GAO analysis of agency reported data. | GAO-19-105

The 23 selected civilian agencies are the Departments of 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.

Although the CIOs for only six agencies reported meeting each of the targets associated with all nine performance indicators for the three cybersecurity CAP goal priority areas, the CIOs at an additional eight agencies reported meeting each target for two of the three priority areas. Specifically,

- one CIO reported that its agency met each of the targets for the (1) information security continuous monitoring and (2) identity, credential, and access management priority areas;
- another CIO reported that its agency met each of the targets for the (1) information security continuous monitoring and (2) anti-phishing and malware defense priority areas; and
- the CIOs at six other agencies met each of the targets for the (1) identity, credential, and access management and (2) anti-phishing and malware defense priority areas.

In fiscal year 2018, the President's Management Agenda[56] replaced the three cybersecurity-focused CAP goal priority areas with updated performance indicators, most of which are to be met by 2020:

1. the **manage asset security** priority area is similar to the information security continuous monitoring priority area from the previous CAP goal and has a focus on understanding the assets and users on agency networks. In addition to hardware asset and software asset management, this priority area includes performance indicators for authorization and mobile device management.
2. the **limit personnel access** priority area focuses on issues of access management. This area includes performance indicators for using automated access management and managing access for privileged network and high-impact system users. The privileged network access management performance indicator is a continuation of the identity, credential, and access management priority area of the previous cybersecurity CAP goal. Therefore, agencies are expected to complete this metric by the end of the fiscal year 2018 FISMA reporting year.

[56] The 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.

3. the **protect networks and data** priority area, which is similar to the anti-phishing and malware defense priority area from the previous cybersecurity CAP goal, has three new performance indicators: intrusion detection and prevention, exfiltration and enhanced defenses, and data protection.

Appendix IV describes the updated cybersecurity-focused CAP priority areas and performance indicators in more detail.

OMB Determined That 13 of the 23 Civilian CFO Act Agencies Were Managing Cybersecurity Risk

In Executive Order 13800, the President directed OMB, in coordination with DHS, to assess and report to the executive branch on the sufficiency and appropriateness of federal agencies' processes for managing cybersecurity risks. For these risk management assessments,[57] OMB leveraged the FISMA metrics reported by agency CIOs and inspectors general for fiscal year 2017. The metrics addressed domains that correspond with the five core security functions identified in the cybersecurity framework. Table 4 lists these domains and their relationship to the core functions.

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

Table 4: *Federal Information Security Modernization Act* Reporting Metric Domains Leveraged by OMB to Assess Agency Risk Management Processes

Core security functions	Domains
Identify	Asset management and authorization Comprehensive risk management
Protect	Remote access protection Credentialing and authorization Network protection
Detect	Anti-phishing capabilities Malware defense capabilities Exfiltration and other capabilities
Respond	Planning and processes Evaluation and Improvement
Recover	Planning and testing Personal impact process Back-up capacity

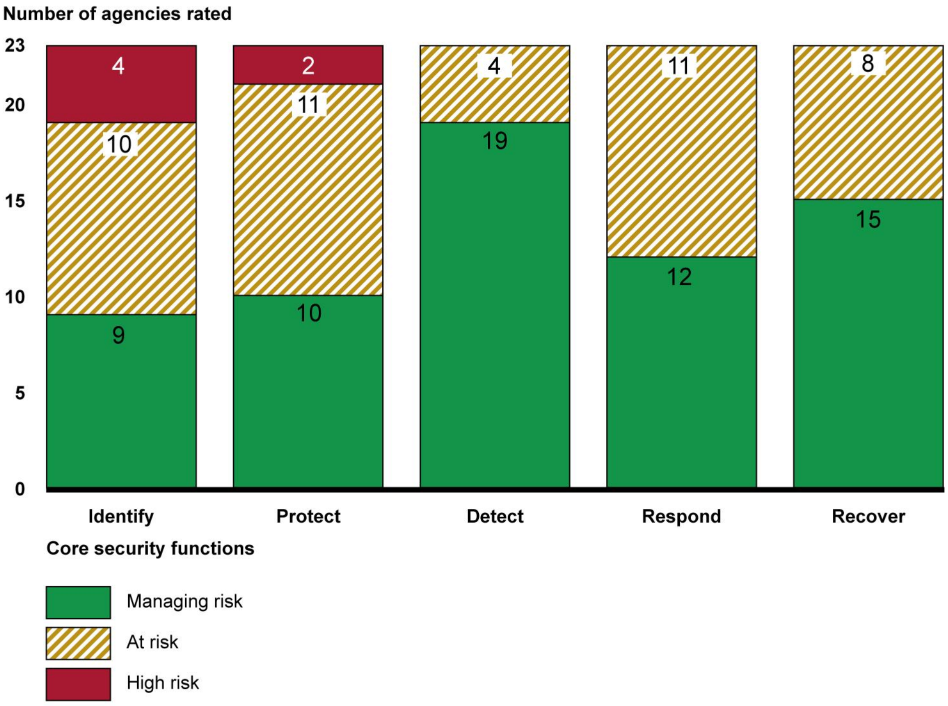
Source: GAO analysis of Office of Management and Budget *Fiscal Year 2017 Federal Information Security Modernization Act of 2014 Annual Report to Congress*. | GAO-19-105

Based on OMB's evaluation of these domains, agency risk management processes related to the five core security functions and overall agency enterprise fell into one of the following three rating categories:

- **managing risk:** required cybersecurity policies, procedures, and tools are in use and the agency actively manages cybersecurity risks;
- **at risk:** some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain; and
- **high risk:** key fundamental cybersecurity policies, processes, and tools are either not in place or not deployed sufficiently.

For fiscal year 2017, OMB reported that not all agencies were managing risk. When considering each of the five core security functions, OMB reported that most of the 23 agencies were at risk or at high risk with regard to the *identify* and *protect* core security functions. Less than half of the 23 agencies were at risk with regard to the *detect*, *respond*, and *recover* core security functions. Overall, OMB determined that 13 agencies were managing risk and that the remaining 10 agencies were at risk of not effectively identifying, protecting, detecting, responding to, and if necessary, recovering from cyber intrusions. Figure 6 shows OMB's risk management assessment ratings by core security function across the 23 agencies for fiscal year 2017.

Figure 6: Risk Management Assessment Ratings by Core Security Function for the 23 Civilian *Chief Financial Officers Act of 1990* Agencies, Fiscal Year 2017



Source: GAO analysis of Office of Management and Budget Fiscal Year 2017 *Federal Information Security Modernization Act of 2014 Annual Report To Congress.* | GAO-19-105

The 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* are the Departments of 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.

DHS and OMB Facilitated the Use of Intrusion Detection and Prevention Capabilities to Secure Federal Agency Systems, but Further Efforts Remain

DHS and OMB, as required by law and policy, have taken various actions to facilitate the agencies' use of intrusion detection and prevention capabilities to secure federal systems. For example, DHS has developed an intrusion assessment plan, deployed NCPS to offer intrusion detection and prevention capabilities to agencies, and is providing tools and services to agencies to monitor their networks through its CDM program. However, NCPS still had limitations in detecting certain types of traffic and agencies were not sending all appropriate traffic through the system. Further, CDM was behind at meeting planned implementation dates, and agencies have requested additional training and guidance for these services. OMB has taken steps to improve upon agencies' capabilities, but has not completed a policy and strategy to do so, or fully reported on its assessment of agencies' capabilities.

DHS Has Taken Actions to Facilitate the Use of Intrusion Detection and Prevention Capabilities and to Make Improvements to Those Capabilities

The *Federal Cybersecurity Enhancement Act of 2015* requires DHS, in coordination with OMB, to develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis. The act also requires that the plan be updated, as necessary.

In December 2016, DHS documented its *Intrusion Assessment Plan*.[58] In the plan, DHS outlined tools, platforms, resources, and ongoing work that the department provides, and that are intended to help agencies detect, identify, and remove intruders on their networks and systems. The intrusion assessment plan also outlines a defense-in-depth strategy, which utilizes multiple layers of cybersecurity and deploys multiple

[58] Department of Homeland Security*, Intrusion Assessment Plan: Fiscal Year 2016 Report to Congress* (Washington, D.C.: Dec. 22, 2016).

capabilities in combination, to secure agencies' networks and information systems. For example, the plan calls for DHS to implement NCPS to provide a perimeter defense for the networks of federal civilian executive branch agencies, while the agencies are to deploy their own intrusion detection and prevention capabilities inside their networks. DHS submitted its intrusion assessment plan to OMB in January 2017.

DHS Has Worked to Improve NCPS, but Agencies Did Not Route All Traffic through Intrusion Detection and Prevention Capabilities Offered by this System

The *Federal Cybersecurity Enhancement Act of 2015* also requires DHS to deploy, operate, and maintain a capability to detect cybersecurity risks and prevent network traffic associated with such risks from transiting to or from an agency information system. In addition, the act requires that DHS make regular improvements to intrusion detection and prevention capabilities by deploying new technologies and modifying existing technologies. Further, the act requires agencies to use this capability on all information traveling between their information systems and any information system other than an agency information system.

DHS developed NCPS, operationally known as EINSTEIN, to provide the capabilities to detect and prevent potentially malicious network traffic from entering agency networks. Consistent with recommendations we made to DHS in January 2016, DHS has taken actions to improve these capabilities and has other actions underway.[59] For example, the department

- determined that enhancing NCPS's current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines would be feasible. In addition, according to DHS officials, the department was operationalizing functionality intended to identify malicious activity in network traffic otherwise missed by signature-based methods.
- determined that developing enhancements to current intrusion detection capabilities to facilitate the scanning of Internet Protocol Version 6 (IPv6)[60] traffic would be feasible. According to DHS officials,

[59] GAO-16-294.

[60] In September 2010, the federal chief information officer issued a memorandum for agency chief information officers stating that the federal government is committed to the operational deployment and use of IPv6, and in July 2012, the Federal Chief Information Officer Council Strategy and Planning Committee issued a roadmap toward IPv6 adoption within the government. The roadmap stated that though both IPv4 (the legacy version of IP) and IPv6 are being used on the Internet, IPv4 is, by far, still the dominate protocol because of its legacy deployment. However, IPv6 traffic growth is inevitable due to the current state of IPv4 address exhaustion, creating an extreme supply and demand curve required to support communications between the U.S. government and its citizens and business partners worldwide.

the department has developed plans to fully support IPv6 for several of its NCPS intrusion detection capabilities. Further, the department has developed implementation schedules and begun roll-out of the enhancements.

- updated the tool it uses to manage and deploy intrusion detection signatures to include a mechanism to clearly link signatures to publicly available, open-source information.
- developed clearly defined requirements for detecting threats on agency internal networks and at cloud service providers to help better ensure effective support of information security activities. According to DHS officials, the department was also continuing pilot activities with cloud service providers to enhance protections of agency assets.
- developed processes and procedures for using vulnerability information, such as data from the CDM program as it becomes available, to help ensure the department is using a risk-based approach for the selection/development of future NCPS intrusion prevention capabilities.

Nevertheless, NCPS continues to have known limitations in its ability to identify potential threats. For example:

- NCPS does not have the ability to effectively detect intrusions across multiple types of traffic. Specifically, DHS determined that developing enhancements to current intrusion detection capabilities to facilitate the scanning of traffic related to supervisory control and data acquisition (SCADA)[61] control systems would not be feasible. However, according to DHS officials, the department is exploring capabilities that are intended to provide critical, cross-sector, real-time visibility into critical infrastructure companies that utilize SCADA systems. In addition, DHS determined that the scanning of encrypted traffic would not be feasible. Nevertheless, according to its officials, the department performed research on potential architectural, technical, and policy mitigation strategies that could provide both the protection and situational awareness for encrypted traffic. The

[61] SCADA is one type of control system, which is a computer-based system used within many infrastructures and industries to monitor and control sensitive processes and physical functions. Control systems perform functions that range from simple to complex. They can be used to simply monitor processes—for example, the environmental conditions in a small office building—or to manage the complex activities of a municipal water system or a nuclear power plant. Control systems are vulnerable to cyberattack from inside and outside the control system network.

department has actions under way to continue its research in this area.

- DHS does not always explicitly ask agencies for feedback or confirmation of receipt of NCPS-related notification. While the department had drafted a standard operating procedure related to its incident notification process, the policy did not instruct DHS analysts specifically to include a solicitation of feedback from agencies within the notification. Further, US-CERT could not provide any information regarding the timetable for when these procedures would take effect.
- Metrics for NCPS, as provided by DHS, do not provide information about how well the system is enhancing government information security or the quality, efficiency and accuracy of supporting actions. Without the deployment of comprehensive measures, DHS cannot appropriately articulate the value provided by NCPS. While the department had taken actions to develop new measures, these measures did not provide a qualitative or quantitative assessment of the system's ability to fulfill the system's objectives.
- NSD did not provide guidance to agencies on how to securely route their information to their Internet service providers. Without providing network routing guidance, NSD has no assurance that the traffic it sees constitutes all or only a subset of the traffic the customer agencies intend to send.

As shown in table 5, as of October 2018, the department had implemented five of the nine recommendations and was in the process of implementing the remainder. However, until DHS completes implementation of the remaining recommendations, the effectiveness of NCPS's intrusion detection and prevention capabilities may be hindered.

Table 5: Status of GAO 2016 Recommendations to Improve the National Cybersecurity Protection System (NCPS) Capabilities as of October 2018[a]

Recommendation	Status	
n/a	Implemented	In process
Determine the feasibility of enhancing NCPS's current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines.	implemented	n/a
Determine the feasibility of developing enhancements to current intrusion detection capabilities to facilitate the scanning of traffic not currently scanned by NCPS.	implemented	n/a
Update the tool the U.S. Computer Emergency Readiness Team uses to manage and deploy intrusion detection signatures to include the ability to more clearly link signatures to publicly available, open-source data repositories.	implemented	n/a
Consider the viability of using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, as an input into the development and management of intrusion detection signatures.	n/a	implemented
Develop a timetable for finalizing the incident notification process, to ensure that customer agencies are being sent notifications of potential incidents, which clearly solicit feedback on the usefulness and timeliness of the notification.	n/a	implemented
Develop metrics that clearly measure the effectiveness of NCPS's efforts, including the quality, efficiency, and accuracy of supporting actions related to detecting and preventing intrusions, providing analytic services, and sharing cyber-related information.	n/a	implemented
Develop clearly defined requirements for detecting threats on agency internal networks and at cloud service providers to help better ensure effective support of information security activities.	implemented	n/a
Develop processes and procedures for using vulnerability information, such as data from the Continuous Diagnostics and Mitigation program as it becomes available, to help ensure DHS is using a risk-based approach for the selection/development of future NCPS intrusion prevention capabilities.	implemented	n/a
Work with customer agencies and the Internet service providers to document secure routing requirements in order to better ensure the complete, safe, and effective routing of information to NCPS sensors.	n/a	implemented

Legend:

✓ A checkmark indicates that the recommendation was either implemented or in the process of being implemented, as designated by the column heading.

Source: GAO analysis of Department of Homeland Security data. | GAO-19-105

[a] Recommendations are found in *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).

In addition, the 23 civilian CFO Act agencies had implemented NCPS capabilities to varying degrees. In a March 2018 report, OMB reported that 21 (about 91 percent) of the 23 agencies had implemented the first two iterations of the NCPS capabilities.[62] In addition, 15 (about 65 percent) of the 23 agencies had implemented all three NCPS capabilities, as shown in table 6 below.[63]

Table 6: Number of Civilian *Chief Financial Officers Act of 1990* Agencies[a] that Had Implemented the National Cybersecurity Protection System Capabilities through EINSTEIN, by Implementation Status, as of September 2017

Capability	Implemented	In progress	Deferred[b]	Not implemented
EINSTEIN 1 / EINSTEIN 2	21	2	0	0
EINSTEIN 3 Accelerated (DNS Sinkholing)[c]	23	0	0	0
EINSTEIN 3 Accelerated (Email Filtering)[d]	15	6	2	0

Source: Office of Management and Budget *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2017*. | GAO-19-105

[a] These summary implementation data aggregate the status for parent agencies based on the lowest implementation status of all of their components.

[b] An agency with a deferred status faced a technical challenge to implement email filtering for its third-party, cloud-based email service. DHS continues to work with the affected agencies and their EINSTEIN 3 Accelerated service provider to engineer solutions.

[c] The Domain Name System (DNS) Sinkholing capability, used to detect and prevent malicious traffic from federal civilian networks, redirects malicious traffic to “safe servers,” also known as “sinkhole” servers.”

[d] The email filtering capability, used to protect against the use of email to deliver malware or induce users to download malware to infect agency networks, scans email destined for federal civilian networks for malicious attachments and other potential cyber threats before being delivered to end-users. According to DHS officials, as of November 2018, the completed number greatly increased since the September 2017 report, with the CFO Act agencies being at 99 percent completed.

However, agencies did not route all network traffic for all information traveling between their information systems and any information system other than an agency information system through NCPS sensors. For

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

[63] While the March 2018 report shows that DHS reported 17 of the 23 civilian CFO Act agencies implementing all three NCPS capabilities, two of the 17 agencies had not fully implemented the EINSTEIN 3 Accelerated Email Filtering capability. Accordingly, we have adjusted this number to reflect the number of agencies that have fully implemented all three capabilities.

example, officials at 13 of 23 agencies stated that not all of their agency external network traffic flowed through NCPS.[64] To illustrate, officials at one agency estimated that 20 percent of their external network traffic did not flow through the system. In addition, 4 of the agencies in our review previously cited several challenges in routing all of their traffic through NCPS intrusion detection sensors, including capacity limitations of the sensors, agreements with external business partners that use direct network connections, interagency network connections that do not route through Internet gateways, use of encrypted communications mechanisms, and backup network circuits that are not used regularly. NSD officials stated that agencies are responsible for routing their traffic to the intrusion detection sensors, and DHS does not have a role in that aspect of NCPS implementation. As a result, potential cyberattacks may not be detected or prevented for a portion of the external traffic at federal agencies. As noted above, we previously recommended that DHS work with agencies to better ensure the complete routing of information to NCPS sensors.

DHS Has Taken Steps to Provide Advanced Network Security Tools, but Has Not Met Planned Implementation Dates

The *Federal Cybersecurity Enhancement Act of 2015* requires DHS to include, in the efforts of the department to continuously diagnose and mitigate cybersecurity risks, advanced network security tools to improve the visibility of network activity and to detect and mitigate intrusions and anomalous activity.

According to DHS officials, the department is addressing the requirement to improve the visibility of network activity by including advanced network security tools as a part of CDM phase 3. In April 2018, we testified that DHS had previously planned to provide 97 percent of federal agencies with the services they needed for CDM phase 3 in fiscal year 2017.[65] In addition, according to OMB's annual FISMA report for fiscal year 2017,

[64] External network traffic (traffic that is routed through agency's external connections) must be routed through a Trusted Internet Connection. External connections include those connections between an agency's information system or network and the globally-addressable Internet or a remote information system or network and networks located on foreign territory.

[65] GAO, *Cybersecurity: DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks*, GAO-18-520T (Washington, D.C.: Apr. 24, 2018).

the CDM program was to continue to incorporate additional capabilities, including phase 3, in fiscal year 2018.[66]

However, DHS now expects initial operational capabilities[67] to be in place for phase 3 in fiscal year 2019. The department has awarded contracts of approximately $3.26 billion to support its Dynamic and Evolving Federal Enterprise Network Defense (also known as DEFEND) aspect of the CDM program, which is to include phase 3. DEFEND also is to provide coverage for existing agency deployments. According to DHS documentation, the task orders associated with DEFEND are to be issued between the second quarter of fiscal year 2018 and the second quarter of fiscal year 2024.

Agencies Indicated the Need for Additional Training and Guidance Related to NCPS and CDM

FISMA requires that DHS provide operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security. Toward this end, DHS has available training and guidance related to the implementation of the capabilities of NCPS (i.e., EINSTEIN) and CDM. Specifically:

- According the DHS officials, the department offers training and guidance to agencies on EINSTEIN 1 implementation. For example, DHS established a program in which the Software Engineering Institute will provide training and mentoring to agencies looking to enhance their understanding of, and proficiency with, the EINSTEIN 1 capability (e.g., network traffic information).[68] NCPS program officials stated that agencies can use this service, which is available at no charge to them, on an unlimited basis as long as the requests relate to EINSTEIN 1. According to the officials, training and guidance related to EINSTEIN 2 and EINSTEIN 3 Accelerated is limited because DHS intentionally restricts the amount of data provided to agencies.

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

[67] Initial operational capability is a DHS-defined project milestone that is attained when the capabilities for a phase have been fully deployed to at least five agencies.

[68] The Software Engineering Institute is a federally funded research and development center at Carnegie Mellon University. The institute works with DHS to strengthen the nation's resistance to cyber threats and improve the practice of cybersecurity.

- According to DHS officials, the department also offers training and guidance to assist agencies with the implementation and use of resources associated with the CDM program, including webinars, guides, and computer-based training. The DEFEND contracts that the department awarded also include a mechanism for agencies to procure specialized tailored training, such as on the use of CDM tools. The department also offers customer advisory forums every other month that agencies are invited to attend. According to CDM program officials, the program's governance, among other topics, is commonly discussed during these forums. Further, the department provides agencies with guidance, such as various governance documents, best practices, and frequently asked questions, through a web portal that is made available by OMB. In addition, US-CERT offers the CDM training program, which is to provide CDM implementation resources.

Nevertheless, most agencies told us that they wanted DHS to provide more training and guidance as it relates to their implementation of the capabilities made available by NCPS and CDM. Specifically,

- Officials from 16 of 23 agencies reported that they wanted to receive additional training on NCPS capabilities. For example, officials at 5 agencies stated that they would like to receive training related to using network traffic information, understanding alerts, or implementing capabilities for cloud services. The officials also stated that they wanted training specific to agency security personnel.
- Officials from 19 of 23 agencies stated that they wanted to receive additional guidance related to NCPS's capabilities, but not all of the 19 provided specific details. For example, officials from at least 3 agencies stated that they wanted additional guidance such as, "how to" documents, descriptions of architecture details, or guidance documents that explain NCPS's capabilities so that agencies can gauge the gap between the security that the system provides and the security being provided by their own agency's capabilities.
- Officials from 21 of 23 agencies reported that they wanted to receive additional training on implementing CDM at their agencies. For example, officials from 7 agencies suggested that additional training on the use of the tools would be beneficial.
- Officials from 22 of 23 agencies stated that they wanted additional guidance as it relates to CDM implementation. For example, officials from one agency stated that they would like examples of best practices and successful deployments.

These requests for additional training and guidance demonstrate that agencies are either unaware of the available training and guidance, or that the training may not meet their needs. Until DHS coordinates with agencies to determine if additional training and guidance are needed, agencies may not be able to fully realize the benefits of the capabilities provided by the NCPS and CDM programs.

OMB Took Actions to Oversee Agency Implementation of Intrusion Detection and Prevention Capabilities and Report to Congress, but Did Not Fully Complete Required Actions

Although OMB took steps to report on agencies' implementation of intrusion detection and prevention capabilities, it did not report on all required actions. For example, the office did not submit DHS's intrusion plan to Congress as required by the *Federal Cybersecurity Enhancement Act of 2015*. In addition, OMB provided various reports to Congress that described agencies' intrusion detection and prevention capabilities, but the reports did not always include all information required by the act. Further, OMB developed a draft policy and strategy that were intended to improve agency capabilities, but it had not finalized these documents.

OMB Did Not Submit the Intrusion Assessment Plan to Congress or Fully Describe the Plan's Implementation in Other Reports

The *Federal Cybersecurity Enhancement Act of 2015* requires OMB to submit the intrusion assessment plan developed by DHS to the appropriate congressional committees no later than 6 months after the date of enactment of the act. The act also required OMB to submit to Congress a description of the implementation of the intrusion assessment plan and the findings of the intrusion assessments[69] conducted pursuant to the intrusion assessment plan no later than 1 year after the date of enactment of the act, and annually thereafter.

Although DHS developed and documented an intrusion assessment plan, which described a defense-in-depth approach to security, OMB did not submit the plan to Congress, as called for in the act. Even though DHS

[69] Intrusion assessments, as defined by the *Federal Cybersecurity Enhancement Act of 2015*, refer to actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems.

submitted the plan to OMB in January 2017, OMB had not submitted it to Congress as of October 2018 (21 months after DHS submitted the plan and 28 months past the due date).

On the other hand, OMB did submit its own reports to Congress which generally described elements of the implementation of DHS's intrusion assessment plan and intrusion assessment findings. In September 2017, OMB issued its analysis of agencies' implementation of intrusion detection and prevention capabilities, or more specifically, agencies' implementation of the various versions of NCPS.[70] In addition, the office's annual FISMA report, issued most recently in March 2018,[71] generally covered elements of the intrusion assessment plan. OMB personnel within the Office of the Federal CIO believed that these two reports, along with a process the office had initiated to validate incidents across the government, addressed the requirement for OMB to submit to Congress a description of the implementation of the intrusion assessment plan and the findings of the intrusion assessments conducted pursuant to the plan.

However, the September 2017 and March 2018 reports did not address other elements described in DHS's intrusion assessment plan. For example, OMB did not describe agency roles associated with segmenting their networks, identifying key servers based on threat and impact, ensuring all applications are appropriately tracked and configured, and categorizing and tagging data based on threat and impact. While OMB has provided important information to congressional stakeholders through its own reports, until it submits the plan and addresses all elements described in DHS's intrusion assessment plan, it will continue to be remiss in providing timely and sufficiently detailed information regarding the intrusion assessment plan to congressional stakeholders to support their oversight responsibilities.

[70] Office of Management and Budget, *Agency Application of the National Cybersecurity Protection System and Intrusion Detection and Prevention Capabilities* (Washington, D.C.: September 2017).

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

OMB Submitted Its Analysis of Agencies' Application of Intrusion Detection and Prevention Capabilities, but Did Not Include the Degree to Which the Capabilities Had Been Applied

The *Federal Cybersecurity Enhancement Act of 2015* also required that OMB submit an analysis of agencies' application of the intrusion detection and prevention capabilities to Congress no later than 18 months after the date of enactment of the act, and annually thereafter. OMB was to include a list of federal agencies and the degree to which each agency had applied the intrusion detection and prevention capabilities in this analysis.

As discussed previously in this report, OMB issued its analysis of agencies' implementation of intrusion detection and prevention capabilities in September 2017. However, the analysis did not include the degree to which agencies had applied the intrusion detection and prevention capabilities. For example, the analysis did not reflect that not all agencies were using this capability on all information traveling between their systems and any system other than an agency system, as required by the act. Until OMB includes the degree to which agencies have applied intrusion detection and prevention capabilities in its analysis, it cannot provide congressional stakeholders with an accurate portrayal of the extent to which the capabilities are detecting and preventing potential intrusions.

The Federal Chief Information Officer Reported on Intrusion Detection and Prevention Capabilities, but Did Not Address All Elements Required by the *Federal Cybersecurity Enhancement Act of 2015*

The *Federal Cybersecurity Enhancement Act of 2015* further required that the Federal Chief Information Officer, within OMB, submit a report to Congress no earlier than 18 months after the date of enactment, but no later than 2 years after that date, assessing the intrusion detection and intrusion prevention capabilities that DHS made available to agencies. The act required that the report address (1) the effectiveness of DHS's system used for detecting, disrupting, and preventing cyber-threat actors, including advanced persistent threats, from accessing agency information and agency information systems; (2) whether the intrusion detection and prevention capabilities, continuous diagnostics and mitigation, and other systems deployed are effective in securing federal information systems; (3) the costs and benefits of the intrusion detection and prevention capabilities, including as compared to commercial technologies and tools, and including the value of classified cyber threat indicators; and (4) the capability of agencies to protect sensitive cyber threat indicators and defensive measures if they were shared through unclassified mechanisms for use in commercial technologies and tools.

In a report issued in September 2018 (about 8 months past the required due date), the Federal Chief Information Officer provided Congress an assessment of intrusion detection and intrusion prevention capabilities across the federal enterprise. The report pointed out, among other things, that agencies did not possess or properly deploy capabilities to detect or prevent intrusions or minimize the impact of intrusions when they occur. In addition, the report acknowledged the need to improve the effectiveness of intrusion detection and intrusion prevention capabilities and stated that OMB would track performance through the CAP goal and annual FISMA reports.

However, the report did not address all of the requirements specified in the act. For example, the report did not address whether DHS's system (i.e., NCPS) was effective in detecting advanced persistent threats. In addition, the report did not include a comparison of the costs and benefits of the intrusion detection and prevention capabilities versus commercial technologies and tools, or the value of classified cyber threat indicators. Further, the report did not address the capability of agencies to protect sensitive cyber threat indicators and defensive measures. Until OMB updates the Federal CIO report to address all of the requirements specified in the act, it will continue to be remiss in providing timely and sufficiently detailed information, such as that related to costs and benefits, among other elements in the act, to congressional stakeholders to support their oversight responsibilities.

OMB Initiated Plans for Improving Agencies' Implementation of Intrusion Detection and Prevention Capabilities, but Has Not Completed a Policy and Strategy

In addition to OMB's responsibilities in the *Federal Cybersecurity Enhancement Act of 2015*, OMB has initiated plans for further improving agencies' intrusion detection and prevention capabilities. In response to a tasking in Executive Order 13800, the Director of the American Technology Council coordinated the development of a report to the President from the Secretary of DHS, the Director of OMB, and the Administrator of the General Services Administration, regarding the modernization of federal information technology (IT).

The report, *Report to the President on Federal IT Modernization*, identified actions that OMB should take for (1) prioritizing the modernization of high-risk, high-value assets and (2) modernizing the Trusted Internet Connection (TIC) program[72] and NCPS to improve protections,[73] remove barriers, and enable commercial cloud migration. For example, OMB was to take the following actions subsequent to the December 13, 2017 report issuance date:

- **Within 60 days:** Update a TIC policy to address challenges with agencies' perimeter-based architectures, such as the modernization of NCPS. In addition, introduce a "90 day sprint" during which approved projects would pilot proposed changes in TIC requirements.
- **Within 90 days:** Update the annual FISMA and CAP goal metrics to focus on those critical capabilities that were most commonly lacking among agencies and focus oversight assessments on high-value assets.
- **Within 120 days:** In conjunction with DHS, develop a strategy for optimally realigning resources across agencies to reduce the risk to high-value assets and respond to cybersecurity incidents for those assets.

OMB has taken steps toward implementing several, but not all, of these actions. For example, it introduced a "90 day sprint" and, according to knowledgeable OMB staff, the outcomes of this action are directly informing changes in TIC requirements. In addition, OMB updated the annual FISMA and CAP goal metrics by including several metrics that focus on high-value assets. The updated FISMA and CAP goal metrics went into effect in April 2018.

[72] In November 2007, OMB issued M-08-05 that announced the Trusted Internet Connections Initiative, which is intended to improve the federal government's security posture by reducing and consolidating external network connections, including Internet connections, currently in use by the government, and by centrally monitoring the traffic passing through these connections for potentially malicious activity. All federal agencies in the executive branch, except for the Department of Defense, are required to implement the initiative. Although the initiative is intended to secure connections to the Internet, other external connections to potentially unsecured systems must also be routed through an approved TIC access point, even if they do not pass through the Internet.

[73] The modernization report notes that TIC gateways apply common security protections for agencies, as well as common intrusion detection, information sharing, and prevention capabilities under DHS's NCPS.

However, while OMB had taken steps toward updating the TIC policy and developing a strategy for optimally realigning resources, the policy and strategy were in draft and had not yet been finalized as of October 2018. The agency did not specify a time frame for finalizing the policy and strategy. Until OMB finalizes the TIC policy and the strategy for optimally realigning resources, the enhancements offered through the policy and strategy are unlikely to be realized.

Selected Agencies Had Not Consistently Implemented Capabilities to Detect and Prevent Intrusions

FISMA requires agencies to provide information security protections to prevent unauthorized access to their systems and information. Officials from the 23 selected agencies reported to us that they generally took steps to meet this requirement by augmenting the tools and services provided by DHS with their own intrusion detection and prevention capabilities. However, agencies did not consistently implement five key capabilities specified by DHS and NIST guidance. In addition, most of the agencies did not fully implement any of the phases of DHS's CDM program that is intended to improve their capabilities to detect and prevent intrusions.

Few Agencies Had Fully Implemented Required Email Protections

Binding Operational Directive (BOD) 18-01 instructs agencies to enhance email security.[74] These enhancements include enabling encrypted email transmission, ensuring that receiving mail servers know what actions the agency would like taken when an email falsely claims to have originated from the agency, and removing certain insecure protocols, among others.[75] The final deadline for implementing all BOD 18-01 requirements was October 16, 2018. Additionally, NIST SP 800-53 Revision 4 recommends that security awareness training include training on how to recognize and prevent spear-phishing attempts.

As of September 2018, only 2 of the 23 agencies reported implementing all of the email requirements. For the remaining 21 agencies:

- 9 agencies stated that their agency had plans to implement all enhancements by the October 2018 deadline,

[74] According to OMB, email, by way of phishing attacks, remains one of the most common threat vectors (or avenues of attack) across the government. See *Federal Cybersecurity Risk Determination Report and Action Plan* (Washington, D.C.: May 2018).

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

- 1 agency was uncertain whether it would meet the deadline, and
- 11 stated they would not be able to meet the deadline.[76]

By contrast, the majority of agencies (22 of 23) reported that they had trained staff on spear-phishing exercises, as recommended by NIST SP 800-53 Revision 4. Officials at the remaining agency told us that the agency planned to have spear-phishing exercises in fiscal year 2019. Such training should help ensure that phishing will be a less effective attack vector against the majority of agencies. While agencies benefit from secure protocols and spear-phishing training, implementing the remaining BOD 18-01 email requirements would provide additional protection to agency information systems.

Agencies Informed GAO That They Often Had Not Implemented Four Key Capabilities

NIST recommends that federal agencies deploy intrusion detection and prevention capabilities. These capabilities include monitoring cloud services, using host-based intrusion prevention systems, monitoring external and internal network traffic, and using a security information and event management (SIEM) system. However, in our semi-structured interviews of the 23 agencies, officials told us that they often had not implemented many of these capabilities. Such inconsistent implementation exposes federal systems and the information they contain to additional risk. As part of their continuing oversight efforts, OMB and DHS can use the information below to work with agencies to identify obstacles and impediments affecting the agencies' abilities to implement these capabilities.

[76] In September 2018, DHS issued a temporary policy exception notice to federal agencies for BOD 18-01's weak email cipher requirement. The notice requested that agencies impacted by the notice submit to DHS preventive security measures and a mitigation strategy that would be in place until these matters would be resolved. Evaluating DHS's temporary policy exception notice and agency actions taken as a result of the notice was not within the scope of this review. Of the 11 agencies that said they would not meet the October 2018 deadline, 4 stated that they could not meet the weak email cipher requirement due to their reliance on external email vendors. Two of the 4 said they were unable to meet other requirements as well.

Less Than Half of the Selected Agencies That Used Cloud Services Monitored Their Cloud-Related Traffic

NIST SP 800-53 Revision 4 states that agencies should monitor and control communications at the external boundary of the network. However, as of June 2018, fewer than half of the agencies that used cloud computing services were monitoring cloud traffic. Specifically:

- 10 of 22 agencies that used Infrastructure as a Service were monitoring inbound and outbound Infrastructure as a Service traffic,
- 7 of 21 agencies that used Platform as a Service were monitoring inbound and outbound Platform as a Service traffic, and
- 10 of 23 agencies that used Software as a Service were monitoring inbound and outbound Software as a Service traffic.

Without monitoring traffic to and from cloud service providers, agencies risk a greater chance of malicious cloud activity detrimentally affecting agency information security.

Several Selected Agencies Had Not Fully Deployed Host-Based Capabilities

NIST SP 800-53 Revision 4 states that agency internal monitoring may be achieved by utilizing intrusion prevention capabilities. These capabilities include using host-based intrusion prevention systems to provide defense at an individual system or device level by protecting against malicious activities. Host-based capabilities include memory-based protection[77] and application whitelisting.[78]

As of June 2018, officials at the 23 agencies reported the following to us:

- 16 agencies used host-based intrusion prevention capabilities,
- 15 agencies used memory-based protection, and
- 8 agencies used host-based application whitelisting.

[77] Memory-based protections are safeguards that protect memory from unauthorized code execution.

[78] An application whitelist is a list of applications and application components that an agency has authorized for use on its hosts.

Until host-based intrusion protections are fully deployed, agencies will be at greater risk of malicious activity adversely affecting agency operations.

Not All Selected Agencies Monitored External and Internal Traffic

NIST SP 800-53 Revision 4 also states that agencies should monitor and control communications at the external boundary of the network and at key internal boundaries (e.g., network traffic). NIST guidance also stated that an agency should deploy monitoring devices strategically within the network to detect essential information.

However, the agencies in our review did not always monitor external and internal traffic. For example, of the 23 agencies:

- 5 reported that they were not monitoring inbound or outbound direct connections to outside entities.
- 11 reported that they were not persistently monitoring inbound encrypted traffic.
- 8 reported that they were not persistently monitoring outbound encrypted traffic.

In addition, 13 agencies reported they were not using a network-based session capture solution.[79] Of the 10 agencies that reported using this solution, officials from 2 agencies stated that they were not capturing workstation-to-workstation connections. Without thorough monitoring of external and internal traffic, agencies will have less assurance that they are aware of compromised or potentially compromised traffic within their network.

Most Agencies Reported Using a Security Information and Event Management Capability, but Did Not Always Use this Capability to Analyze Potential Threats

NIST SP 800-53 Revision 4 states that agencies should establish enhanced monitoring capabilities. Such capabilities should include automated mechanisms that collect and analyze incident data for increased threat and situational awareness. According to NIST, a security information and event management (SIEM) system analyzes data from

[79] A network-based session capture solution records information exchanged across an agency's network.

different sources and identifies and prioritizes significant events. Sources of data used by SIEM systems include logs from database systems, network devices, security systems, web applications, and workstation operating systems.[80]

Of the 23 agencies that we reviewed, 21 reported using a SIEM capability. Over half of the agencies employing a SIEM used one or more of their logs to match against known vulnerabilities and advanced persistent threats, as well as to create real-time alerts. For example, of the 21 agencies:

- 14 agencies reported collecting database logs, but only 7 agencies reported using the logs to match against known vulnerabilities and persistent threats and to create real-time alerts;
- 20 agencies reported collecting network logs, but only 13 agencies reported using them to match against known vulnerabilities and persistent threats and to create real-time alerts;
- 21 agencies reported collecting security logs, but only 13 reported using them to match against known vulnerabilities and persistent threats and to create real-time alerts;
- 15 agencies reported collecting web application logs, but only 9 agencies reported using them to match against known vulnerabilities and persistent threats and to create real-time alerts; and
- 13 agencies reported collecting workstation logs, but only 8 agencies reported using them to match against known vulnerabilities and persistent threats and to create real-time alerts.
- Only 5 agencies collected all 5 types of logs and used them to match against known vulnerabilities and persistent threats and to create real-time alerts.

By not fully using SIEM capabilities, agencies will have less assurance that relevant personnel will be aware of possible weaknesses or intrusions.

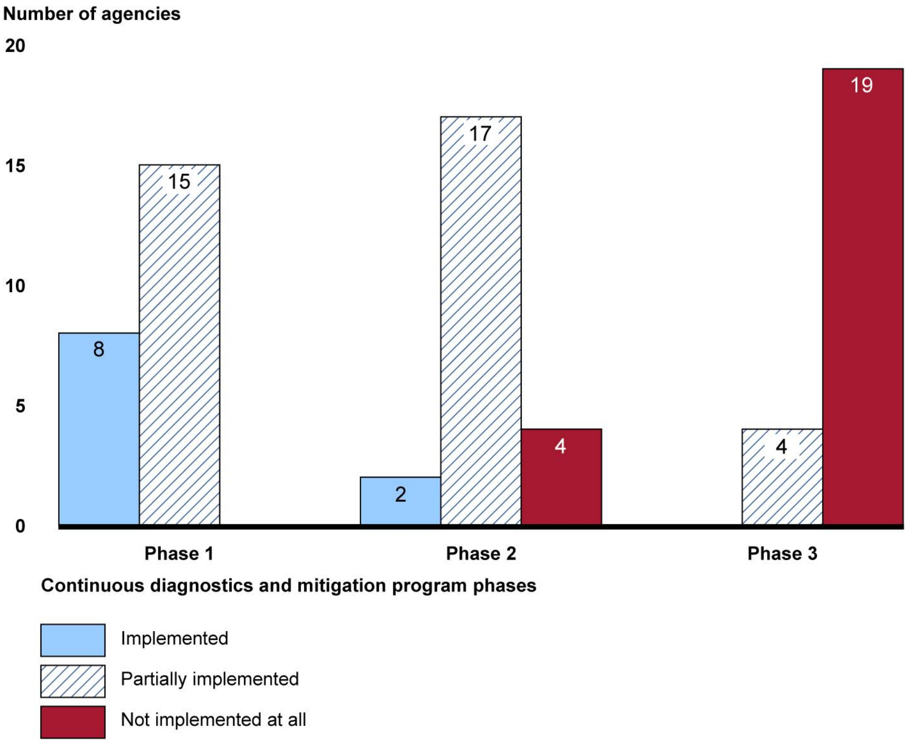
[80] According to NIST, logs are records of the events occurring within an organization's systems and networks. Logs from security software, operating systems, and applications typically contain information that includes security-related data.

Agencies Are in the Process of Implementing DHS' CDM Program, but Most Agencies Have Not Fully Implemented Any of the Program Phases

To further enhance their intrusion detection and prevention capabilities, the 23 civilian CFO Act agencies were in the process of implementing DHS's CDM program. As previously discussed, Phase 1 of the program involves deploying products to automate hardware and software asset management, configuration settings, and common vulnerability management capabilities. Phase 2 intends to address privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. Phase 3 is intended to assess agency network activity and identify any anomalies that may indicate a cybersecurity compromise.

As of June 2018, most agencies had not fully implemented any of the three phases. As shown in Figure 7, 15 agencies had partially implemented phase 1, 21 had partially or not yet begun to implement phase 2, and none of the agencies had fully implemented phase 3.

Figure 7: Civilian *Chief Financial Officers Act of 1990* Agencies' Implementation of DHS's Continuous Diagnostics and Mitigation Program Phases, as of June 2018



Source: GAO analysis based on agency provided data. | GAO-19-105

Agencies' implementation status has been affected, at least in part, due to delays in DHS's deployment of the program phases. As a result, federal systems will remain at risk until the program is fully deployed.

Conclusions

Many agencies have not effectively implemented the federal approach and strategy for securing information systems. For example, the inspectors general for 17 of the 23 selected agencies reported that their agencies had not effectively implemented their information security programs and had significant information security deficiencies associated with internal control over financial reporting. In addition, CIOs for 17 agencies reported not meeting all nine targets for the cybersecurity cross-agency priority goal. Further, OMB determined that that only 13 of the 23 agencies were managing risks to their overall enterprise, while the other

10 agencies were at risk. Until agencies more effectively implement the government's approach and strategy, federal systems will remain at risk.

DHS and OMB have initiatives underway that are intended to further improve agencies' security posture. However, although DHS had provided training and guidance for NCPS and CDM, agencies expressed the need for more. In addition, OMB had also not finalized its policy and strategy aimed at addressing challenges with perimeter security and protecting high value assets, respectively. OMB had also not provided useful information to Congress, such as a description of agencies' implementation of DHS's intrusion assessment plan, the degree to which agencies are using NCPS, a complete analysis of agencies' implementation of DHS's intrusion assessment plan, or the costs and benefits of using commercial tools.

Although agencies' officials reported various efforts underway to enhance their agency's intrusion detection and prevention capabilities, implementation efforts across the federal government were not consistent. OMB and DHS can use the information provided in this report to work with agencies to identify obstacles and impediments affecting the agencies' abilities to implement these capabilities.

Recommendations for Executive Action

We are making a total of nine recommendations, including two to DHS and seven to OMB. Specifically:

- The Secretary of DHS should direct the Network Security Deployment division to coordinate further with federal agencies to identify training and guidance needs for implementing NCPS and CDM. (Recommendation 1)
- The Secretary of DHS should direct the appropriate staff to work with OMB to follow up with agencies to identify obstacles and impediments affecting their abilities to implement intrusion detection and prevention capabilities. (Recommendation 2)
- The Director of OMB should submit the intrusion assessment plan to the appropriate congressional committees. (Recommendation 3)
- The Director of OMB should report on implementation of the defense-in-depth strategy described in the intrusion assessment plan, including all elements described in the plan. (Recommendation 4)

- The Director of OMB should update the analysis of agencies' intrusion detection and prevention capabilities to include the degree to which agencies are using NCPS. (Recommendation 5)
- The Director of OMB should direct the Federal CIO to update her report to Congress to include required information, such as detecting advanced persistent threats, a comparison of the costs and benefits of the capabilities versus commercial technologies and tools, and the capability of agencies to protect sensitive cyber threat indicators and defense measures. (Recommendation 6)
- The Director of OMB should establish a time frame for finalizing the Trusted Internet Connections policy intended to address challenges with agencies' perimeter-based architectures and issue it when finalized. (Recommendation 7)
- The Director of OMB should establish a time frame for finalizing the strategy for realigning resources across agencies to protect high-value assets and issue it when finalized. (Recommendation 8)
- The Director of OMB should direct the Federal CIO to work with DHS to follow-up with agencies to identify obstacles and impediments affecting their abilities to implement intrusion detection and prevention capabilities. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report to OMB and the 23 civilian CFO Act agencies, including DHS, covered by our review. In response, OMB provided comments via email, and DHS and three other agencies (the Department of Commerce, Social Security Administration, and U.S. Agency for International Development) provided written comments, which are reprinted in appendices V through VIII, respectively. The 19 remaining agencies (the Departments of Agriculture, Education, Energy, Health and Human Services, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; as well as the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, and Small Business Administration) stated via email that they had no comments.

In its comments, which the OMB liaison provided to GAO via email on December 7, 2018, OMB did not state whether it agreed or disagreed with the seven recommendations that we made to it. Rather, according to the liaison, OMB agreed with the facts in our draft report, but found that the report did not reflect the agency's rationale for not submitting the DHS intrusion assessment plan to Congress and a report on the implementation of the plan, as required by the *Federal Cybersecurity Enhancement Act of 2015*. The liaison stated that OMB is working closely with DHS to provide strategic direction in assessing gaps in, and modernizing, the manner in which intrusion detection and prevention capabilities are delivered to the federal government. Further, in a subsequent email on December 10, 2018, OMB said it believes the Federal CIO's September 2018 report to Congress, along with data provided in OMB's fiscal year 2017 FISMA report to Congress, achieves the outcomes sought by the *Federal Cybersecurity Enhancement Act of 2015* and demonstrates OMB's continuous engagement with DHS across the evolution of the intrusion detection and prevention program.

As stated in our report, we acknowledge that OMB has provided important information to congressional stakeholders through its reports. However, OMB's reports did not cover all outcomes described in the act. For example, as we pointed out, these reports did not fully address implementation of the defense-in-depth strategy described in DHS's intrusion assessment plan. In addition, although OMB reported on several elements required by the *Federal Cybersecurity Enhancement Act of 2015*, it did not report on all of the required elements. For example, the reports did not address whether DHS's NCPS was effective in detecting advanced persistent threats. The reports also did not include a comparison of the costs and benefits of the intrusion detection and prevention capabilities versus commercial technologies and tools, or the value of classified cyber threat indicators. Further, the reports did not address the capability of agencies to protect sensitive cyber threat indicators and defensive measures. Accordingly, we maintain that our recommendations for OMB to report on required elements in the *Federal Cybersecurity Enhancement Act of 2015* are warranted.

In addition, OMB suggested that we revise our recommendations to the agency to include a shared responsibility with DHS to help drive desired outcomes. However, six of the seven recommendations we are making to OMB are related to specific OMB responsibilities cited in either the *Federal Cybersecurity Enhancement Act of 2015* or the *Report to the President on Federal IT Modernization*. As such, we believe the recommendations are appropriately addressed to OMB. Furthermore, our recommendations do not prevent OMB from working with DHS to implement them. Our seventh recommendation to OMB—to work with DHS to follow up with agencies to identify obstacles and impediments affecting their abilities to implement intrusion detection and prevention capabilities—includes a shared responsibility with DHS. OMB also provided technical comments, which we incorporated into the report, as appropriate.

Subsequent to providing initial comments on our draft report, OMB issued a memorandum intended to provide a strategy for realigning resources across agencies to protect high-value assets.[81] This action addresses our recommendation 8, which called for the Director of OMB to establish a time frame for finalizing the strategy for realigning resources across agencies to protect high-value assets, and to issue the strategy when finalized.

In its comments, DHS stated that it concurred with the two recommendations we made to the department. DHS stated that it expects to implement the recommendations in 2019.

The Department of Commerce commented that the report was reasonable and that the department agreed with the findings and recommendations.

In its comments, the Social Security Administration stated that protecting its networks and information is a critical priority. According to the agency, it continued to make improvements in fiscal year 2018, such as improvements and progress in securing applications, leveraging the cloud, managing its assets and vulnerabilities, strengthening its network and incident response capabilities, improving its security training, and enhancing the overall effectiveness of its cybersecurity program.

Finally, the U.S. Agency for International Development commented that its inspector general had improved the agency's capability maturity ratings for core security functions in fiscal year 2018. The agency also pointed out that it was the only selected agency in which fiscal year 2017 indicators of effectiveness in implementing the federal approach and strategy for securing information systems were all positive (as noted in Appendix III).

[81] Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

We are sending copies of this report to appropriate congressional committees, the Director of OMB, the heads of the 23 civilian CFO Act agencies and their inspectors general, 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 IX.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The *Federal Cybersecurity Enhancement Act of 2015*, which was enacted December 18, 2015, included a provision for GAO to report on the effectiveness of the federal government's approach and strategy for securing agency information systems, including intrusion detection and prevention capabilities.[1] The objectives of our review were to assess: (1) the reported effectiveness of selected agencies' implementation of the federal government's approach and strategy to securing agency information systems; (2) the extent to which the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) have facilitated the use of intrusion detection and prevention capabilities to secure federal agency information systems; and (3) the extent to which selected agencies reported implementing intrusion detection and prevention capabilities.

Selected agencies for our review were the 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act).[2] We did not include the Department of Defense because the *Federal Cybersecurity Enhancement Act of 2015* only pertains to civilian agencies. Because we focused our work on the 23 civilian agencies, results from these reviews are not generalizable to the entire federal government.

To assess the reported effectiveness of agencies' implementation of the federal government's approach and strategy to securing agency information systems, we

[1] The act is a part of the *Consolidated Appropriations Act*, 2016, Pub. L. No. 114-113, div. N, title II, subtitle B, 129 Stat. 2242, 2963 -2975 (Dec. 18, 2015).

[2] The 23 civilian *Chief Financial Officers Act of 1990* agencies are the Departments of 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.

- described the federal government's approach and strategy by summarizing the *Federal Information Security Modernization Act of 2014* (FISMA),[3] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[4] and the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[5] (cybersecurity framework).
- assessed the reported effectiveness of agencies' implementation of the approach and strategy by reviewing annual reports from OMB and the inspectors general (IG) of the 23 civilian CFO Act agencies regarding the reported implementation of FISMA for fiscal year 2017. We described the IG reported maturity levels, including the *Office of Inspectors General FISMA Reporting Metrics* definition of "effectiveness." These maturity levels are based on security domains aligned with the five core functions in NIST's cybersecurity framework. We also summarized IG reported conclusions on the effectiveness of agencies' information security programs for fiscal year 2017.
- reviewed the fiscal year 2016 and 2017 financial statement audit reports for each of the 23 civilian CFO Act agencies to identify the extent to which any significant deficiencies or material weaknesses related to information security over financial systems had been reported and to identify information security control weaknesses reported by the IGs.
- identified whether agencies had met the targets for the cybersecurity-focused cross-agency priority goal for fiscal years 2016 and 2017 by examining agency-reported performance metrics for fiscal years 2016 and 2017.

[3] The *Federal Information Security Modernization Act of 2014* (FISMA 2014), enacted as Pub. L. No. 113-283, 128 Stat. 3073 (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 both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[4] The 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).

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

- evaluated OMB's agency risk management assessment ratings to make a determination on how agencies were managing risk to their enterprise. These conclusions were based on FISMA metrics, and are aligned with the five core security functions defined in the cybersecurity framework.
- interviewed knowledgeable OMB officials and staff to obtain their views on the reported effectiveness of the federal government's approach and strategy to securing agency information systems.

To assess the extent to which OMB and DHS have facilitated the use of intrusion detection and prevention capabilities to secure federal agency information systems, we

- determined the extent OMB and DHS fulfilled their requirements described in the *Federal Cybersecurity Enhancement Act of 2015* by collecting and reviewing artifacts from OMB and DHS and comparing them to the provisions outlined in the act. We also interviewed knowledgeable officials from OMB and DHS regarding their efforts to fulfill their requirements described in the act.
- determined the effectiveness of corrective actions taken by DHS to address nine previously reported recommendations we made in our report related to NCPS.[6] Specifically, we collected appropriate artifacts and assessed the artifacts against the criteria used in that report, and determined the extent to which the actions taken by DHS met the intent of the recommendations, and we met with DHS staff responsible for the remediation activities and obtained their views of the status of actions taken to address the recommendations.
- held semi-structured interviews[7] with knowledgeable officials from the 23 civilian CFO Act agencies. During these interviews, we obtained the agency's views on whether they need more training and guidance from DHS for NCPS and CDM. We also interviewed knowledgeable officials and staff at DHS to obtain their views on how DHS had improved the intrusion detection and prevention capabilities it

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

[7] A semi-structured interview methodology generally involves asking a similar subset of questions of multiple interviewees. We used a semi-structured interview format with both closed- and open-ended questions. The intent of our open-ended questions was to engage the agency officials in a conversation about the topics being discussed.

provides to federal agencies. We also interviewed DHS officials to obtain their views on the training and guidance that the department makes available to agencies.

To assess the extent to which selected agencies reported implementing intrusion detection and prevention capabilities, we described the reported intrusion detection and prevention capabilities implemented by the 23 civilian CFO Act civilian agencies by

- summarizing implemented intrusion detection and prevention capability information obtained from the semi-structured interviews at the 23 civilian CFO Act agencies described above;
- identifying the extent to which the 23 civilian CFO Act agencies were in compliance with DHS's binding operating directive (BOD) pertaining to enhanced email and web security (BOD 18-01) by collecting and summarizing *Cyber Hygiene Trustworthy Email* reports from the 23 agencies and determining the extent to which the agencies had taken required actions to implement the BOD.

During the semi-structured interviews, we also obtained the agency's views and experiences with other programs and services provided by DHS, including the extent to which agencies had implemented the tools offered by the department's Continuous Diagnostics and Mitigation (CDM) program.

To determine the reliability of submitted data and obtain clarification about agencies' processes to ensure the accuracy and completeness of data used in their respective FISMA reports, we analyzed documents and conducted interviews with officials from 6 of the 23 civilian CFO Act agencies. To select these six agencies, we sorted agency fiscal year 2017 information technology budget data from highest to lowest amount and then divided the data into three tiers: high spending, medium spending, and low spending. We then randomly selected two agencies from each of the three tiers. The selected agencies were the Departments of Agriculture, Commerce, Housing and Urban Development, Transportation, and Veterans Affairs, and the U.S. Agency for International Development. While not generalizable to all agencies, the information we collected and analyzed about the six selected agencies provided insights into various processes in place to produce FISMA reports. Based on this assessment, we determined that the data were sufficiently reliable for the purposes of our reporting objectives.

We conducted this performance audit from December 2017 to December 2018 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 7.

Table 7: National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity

Category	Subcategory
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.
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-2: Software platforms and applications within the organization are inventoried.
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-3: Organizational communication and data flows are mapped.

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

Category	Subcategory
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-4: External information systems are catalogued.
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-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
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-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
Identify (ID) core function: 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.
Identify (ID) core function: 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-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.
Identify (ID) core function: 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-3: Priorities for organizational mission, objectives, and activities are established and communicated.
Identify (ID) core function: 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-4: Dependencies and critical functions for delivery of critical services are established.

Category	Subcategory
Identify (ID) core function: 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-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational cybersecurity policy is established and communicated.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, 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.
Identify (ID) core function: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-4: Governance and risk management processes address cybersecurity risks.
Identify (ID) core function: 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.
Identify (ID) core function: 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-2: Cyber threat intelligence is received from information sharing forums and sources.

Category	Subcategory
Identify (ID) core function: 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-3: Threats, both internal and external, are identified and documented.
Identify (ID) core function: 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-4: Potential business impacts and likelihoods are identified.
Identify (ID) core function: 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-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
Identify (ID) core function: 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-6: Risk responses are identified and prioritized.
Identify (ID) core function: 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.
Identify (ID) core function: 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-2: Organizational risk tolerance is determined and clearly expressed.
Identify (ID) core function: 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-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.
Identify (ID) core function: 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.

Category	Subcategory
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-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.
Identify (ID) core function: 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-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.

Category	Subcategory
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-2: Physical access to assets is managed and protected.
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-3: Remote access is managed.
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-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
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-5: Network integrity is protected (e.g., network segregation, network segmentation).
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-6: Identities are proofed and bound to credentials and asserted in interactions.
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-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)

Category	Subcategory
Protect (PR) core function: 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.
Protect (PR) core function: 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-2: Privileged users understand their roles and responsibilities.
Protect (PR) core function: 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-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
Protect (PR) core function: 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-4: Senior executives understand their roles and responsibilities.
Protect (PR) core function: 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-5: Physical and cybersecurity personnel understand their roles and responsibilities.
Protect (PR) core function: 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.
Protect (PR) core function: 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-2: Data-in-transit is protected.
Protect (PR) core function: 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-3: Assets are formally managed throughout removal, transfers, and disposition.

Category	Subcategory
Protect (PR) core function: 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-4: Adequate capacity to ensure availability is maintained.
Protect (PR) core function: 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-5: Protections against data leaks are implemented.
Protect (PR) core function: 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-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
Protect (PR) core function: 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-7: The development and testing environment(s) are separate from the production environment.
Protect (PR) core function: 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-8: Integrity checking mechanisms are used to verify hardware integrity.
Protect (PR) core function: 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).
Protect (PR) core function: 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-2: A System Development Life Cycle to manage systems is implemented.

Category	Subcategory
Protect (PR) core function: 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-3: Configuration change control processes are in place.
Protect (PR) core function: 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-4: Backups of information are conducted, maintained, and tested.
Protect (PR) core function: 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-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
Protect (PR) core function: 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-6: Data is destroyed according to policy.
Protect (PR) core function: 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-7: Protection processes are improved.

Category	Subcategory
Protect (PR) core function: 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-8: Effectiveness of protection technologies is shared.
Protect (PR) core function: 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-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
Protect (PR) core function: 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-10: Response and recovery plans are tested.
Protect (PR) core function: 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-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
Protect (PR) core function: 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-12: A vulnerability management plan is developed and implemented.
Protect (PR) core function: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.

Category	Subcategory
Protect (PR) core function: Maintenance (PR.MA): Maintenance and repairs of industrial control and information 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.
Protect (PR) core function: 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.
Protect (PR) core function: 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-2: Removable media is protected and its use restricted according to policy.
Protect (PR) core function: 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-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
Protect (PR) core function: 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-4: Communications and control networks are protected.
Protect (PR) core function: 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-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.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-4: Impact of events is determined.

Category	Subcategory
Detect (DE) core function: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-5: Incident alert thresholds are established.
Detect (DE) core function: 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.
Detect (DE) core function: 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-2: The physical environment is monitored to detect potential cybersecurity events.
Detect (DE) core function: 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-3: Personnel activity is monitored to detect potential cybersecurity events.
Detect (DE) core function: 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-4: Malicious code is detected.
Detect (DE) core function: 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-5: Unauthorized mobile code is detected.
Detect (DE) core function: 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-6: External service provider activity is monitored to detect potential cybersecurity events.
Detect (DE) core function: 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-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
Detect (DE) core function: 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-8: Vulnerability scans are performed.
Detect (DE) core function: 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.

Category	Subcategory
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-2: Detection activities comply with all applicable requirements.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-3: Detection processes are tested.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4: Event detection information is communicated.
Detect (DE) core function: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	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.
Respond (RS) core function: 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.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-2: Incidents are reported consistent with established criteria.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-3: Information is shared consistent with response plans.
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.

Category	Subcategory
Respond (RS) core function: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-2: The impact of the incident is understood.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-3: Forensics are performed.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-4: Incidents are categorized consistent with response plans.
Respond (RS) core function: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	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).
Respond (RS) core function: 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.
Respond (RS) core function: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-2: Incidents are mitigated.
Respond (RS) core function: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
Respond (RS) core function: 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.
Respond (RS) core function: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-2: Response strategies are updated.

Category	Subcategory
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.
Recover (RC) core function: Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.
Recover (RC) core function: Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-2: Recovery strategies are updated.
Recover (RC) core function: 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 CSIRTs, and vendors).	RC.CO-1: Public relations are managed.
Recover (RC) core function: 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 CSIRTs, and vendors).	RC.CO-2: Reputation is repaired after an incident.
Recover (RC) core function: 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 CSIRTs, and vendors).	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-19-105

Appendix III: Reported Effectiveness of Agencies' Implementation of the Federal Approach for Securing Information Systems

The federal approach and strategy for securing information systems is prescribed by federal law and policy, including the *Federal Information Security Modernization Act of 2014*[1] and the presidential executive order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[2] Accordingly, federal reports describing agency implementation of this law and policy, and reports of related agency information security activities, indicated the effectiveness of agencies' efforts to implement the federal approach and strategy. Table 8 summarizes the reported effectiveness of the 23 civilian *Chief Financial Officers Act of 1990* agencies to implement the government's approach and strategy to securing information systems.

Table 8: Fiscal Year 2017 Indicators of the 23 Selected Civilian *Chief Financial Officers Act of 1990* Agencies' Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems

Agency	Inspector General Information Security Program Ratings	Inspector General Internal Control Deficiencies over Financial Reporting	CIO Cybersecurity Cross-Agency Priority Goal Targets	OMB Risk Management Assessment Ratings
US Department of Agriculture	Not effective	Material weakness	Not met	At risk
Department of Commerce	Not effective	Significant deficiency	Not met	At risk

[1] The *Federal Information Security Modernization Act of 2014*, enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002*, enacted as *Title III, E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[2] The 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).

Agency	Inspector General Information Security Program Ratings	Inspector General Internal Control Deficiencies over Financial Reporting	CIO Cybersecurity Cross-Agency Priority Goal Targets	OMB Risk Management Assessment Ratings
Department of Education	Not effective	Significant deficiency	Met	Managing risk
Department of Energy	Effective	—	Not met	At risk
Department of Health and Human Services	Not effective	Material weakness	Not met	At risk
Department of Homeland Security	Effective	Material weakness	Not met	Managing risk
Department of Housing and Urban Development	Not effective	Significant deficiency	Met	Managing risk
Department of the Interior	Not effective	Significant deficiency	Not met	Managing risk
Department of Justice	Not effective	—	Not met	Managing risk
Department of Labor	Not effective	Significant deficiency	Not met	Managing risk
Department of State	Not effective	Significant deficiency	Not met	At risk
Department of Transportation	Not effective	—	Not met	At risk
Department of the Treasury	Not effective	Material weakness	Not met	Managing risk
Department of Veterans Affairs	Not effective	Material weakness	Not met	At risk
Environmental Protection Agency	Effective	Significant deficiency	Not met	At risk
General Services Administration	Not effective	Significant deficiency	Met	Managing risk
National Aeronautics and Space Administration	Not effective	Significant deficiency	Not met	At risk
National Science Foundation	Effective	—	Not met	Managing risk
Nuclear Regulatory Commission	Effective	—	Not met	Managing risk
Office of Personnel Management	Not effective	Material weakness	Met	Managing risk
Small Business Administration	Not effective	Significant deficiency	Not met	At risk
Social Security Administration	Not effective	Significant deficiency	Met	Managing risk
US Agency for International Development	Effective	—	Met	Managing risk
Totals[a]	**17**[b]	**17**[c]	**17**[d]	**10**[e]

Legend: "—" means that information security was not designated as a significant deficiency or material weakness for that agency.

Source: GAO analysis based on agency and Office of Management and Budget fiscal year 2017 *Federal Information Security Modernization Act* data and agency financial reports for fiscal year 2017. | GAO-19-105

[a] Although the totals for some of the columns are the same, the agencies included in the totals are not.

[b] The inspector general for 17 agencies reported that their agency did not have an effective information security program.

[c] The inspector general for 17 agencies designated information security as a significant deficiency or material weakness.

[d] The chief information officers for 17 agencies reported that their agencies did not meet all nine targets for the cybersecurity cross-agency priority goal.

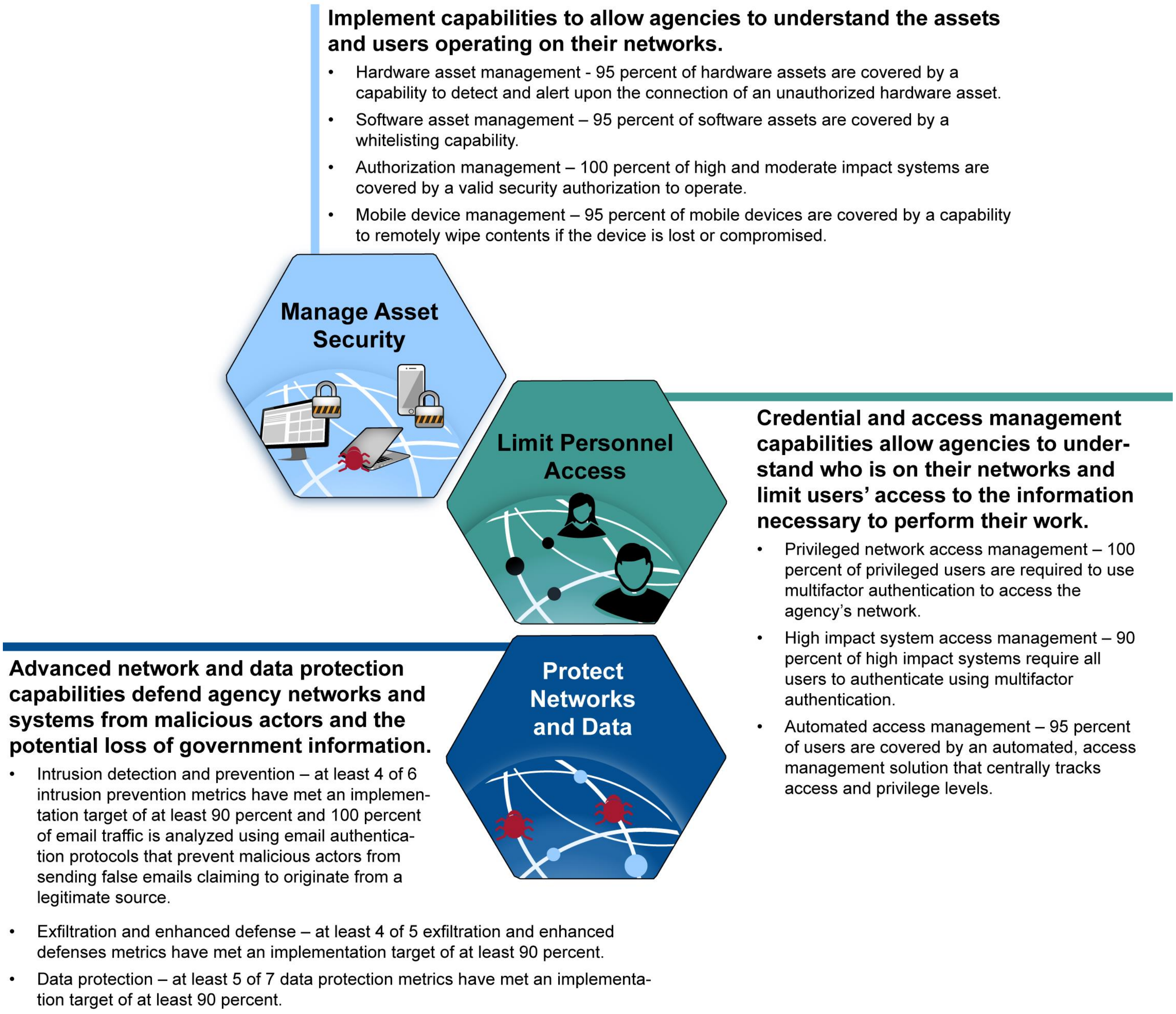
[e] OMB reported that 10 agencies had enterprises that were at risk.

Appendix IV: Updated Cybersecurity-Focused Cross-Agency Priority Goal

The President’s Management Agenda identifies cross-agency priority (CAP) goals to target areas where multiple agencies must collaborate to effect change.[1] The agenda issued in fiscal year 2018 established an information technology modernization goal that includes a cybersecurity objective with specific priority areas and performance indicators. This cybersecurity-focused goal is intended to drive progress in the government’s efforts to modernize information technology to increase productivity and security. Figure 8 describes the 3 updated cybersecurity-focused cross-agency priority areas and 10 performance indicators. Each federal agency is expected to meet one of the 10 new performance indicators by the end of fiscal year 2018 and the remainder by 2020.

[1] The 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.

Figure 8: Cybersecurity-Focused Cross-Agency Priority Goal Priority Areas and Performance Indicators, Fiscal Years 2018–2022



Implement capabilities to allow agencies to understand the assets and users operating on their networks.

- Hardware asset management - 95 percent of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.
- Software asset management – 95 percent of software assets are covered by a whitelisting capability.
- Authorization management – 100 percent of high and moderate impact systems are covered by a valid security authorization to operate.
- Mobile device management – 95 percent of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.

Credential and access management capabilities allow agencies to understand who is on their networks and limit users' access to the information necessary to perform their work.

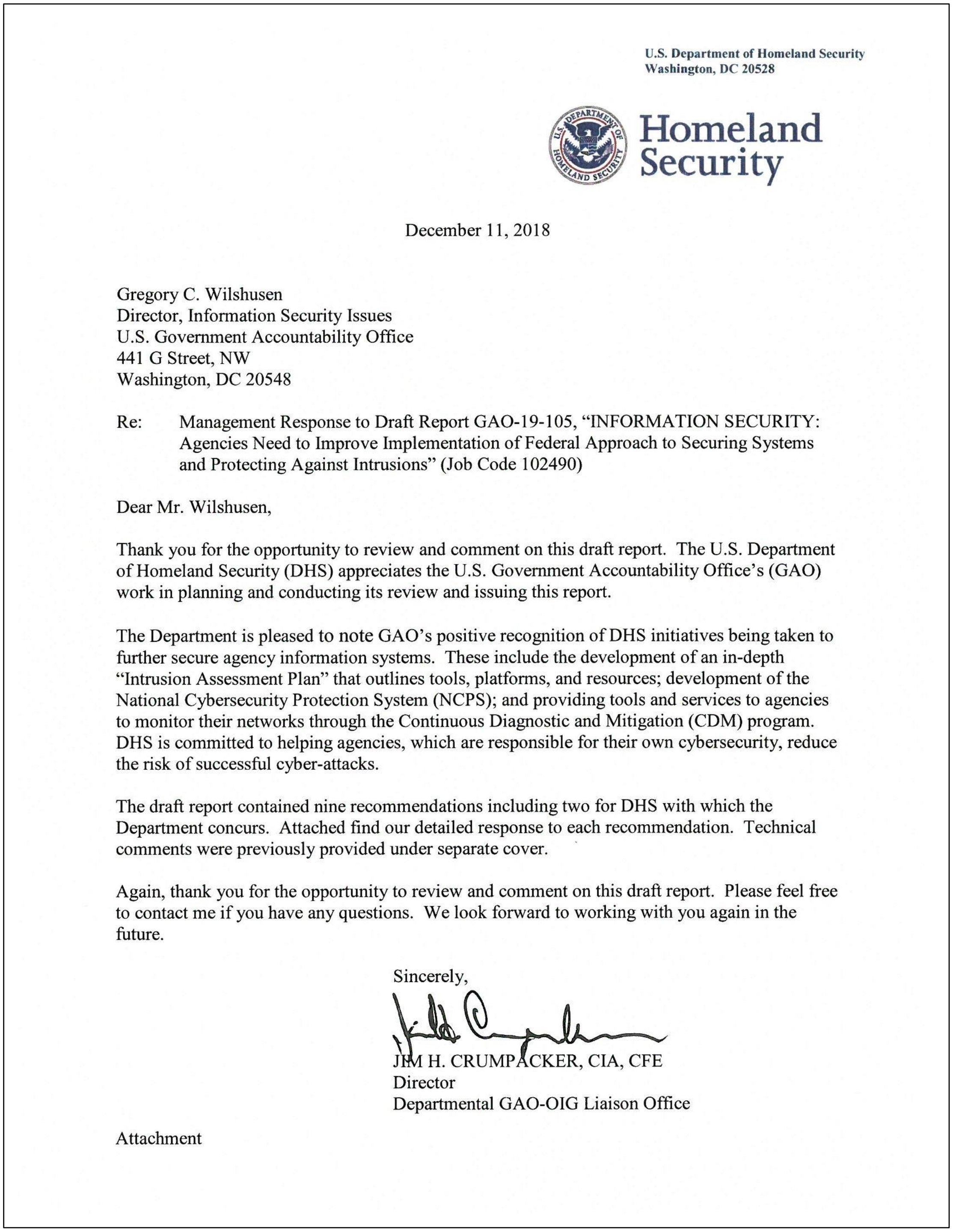
- Privileged network access management – 100 percent of privileged users are required to use multifactor authentication to access the agency's network.
- High impact system access management – 90 percent of high impact systems require all users to authenticate using multifactor authentication.
- Automated access management – 95 percent of users are covered by an automated, access management solution that centrally tracks access and privilege levels.

Advanced network and data protection capabilities defend agency networks and systems from malicious actors and the potential loss of government information.

- Intrusion detection and prevention – at least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90 percent and 100 percent of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.
- Exfiltration and enhanced defense – at least 4 of 5 exfiltration and enhanced defenses metrics have met an implementation target of at least 90 percent.
- Data protection – at least 5 of 7 data protection metrics have met an implementation target of at least 90 percent.

Source: Performance.gov. | GAO-19-105

Appendix V: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 11, 2018

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

Re: Management Response to Draft Report GAO-19-105, "INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions" (Job Code 102490)

Dear Mr. Wilshusen,

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of DHS initiatives being taken to further secure agency information systems. These include the development of an in-depth "Intrusion Assessment Plan" that outlines tools, platforms, and resources; development of the National Cybersecurity Protection System (NCPS); and providing tools and services to agencies to monitor their networks through the Continuous Diagnostic and Mitigation (CDM) program. DHS is committed to helping agencies, which are responsible for their own cybersecurity, reduce the risk of successful cyber-attacks.

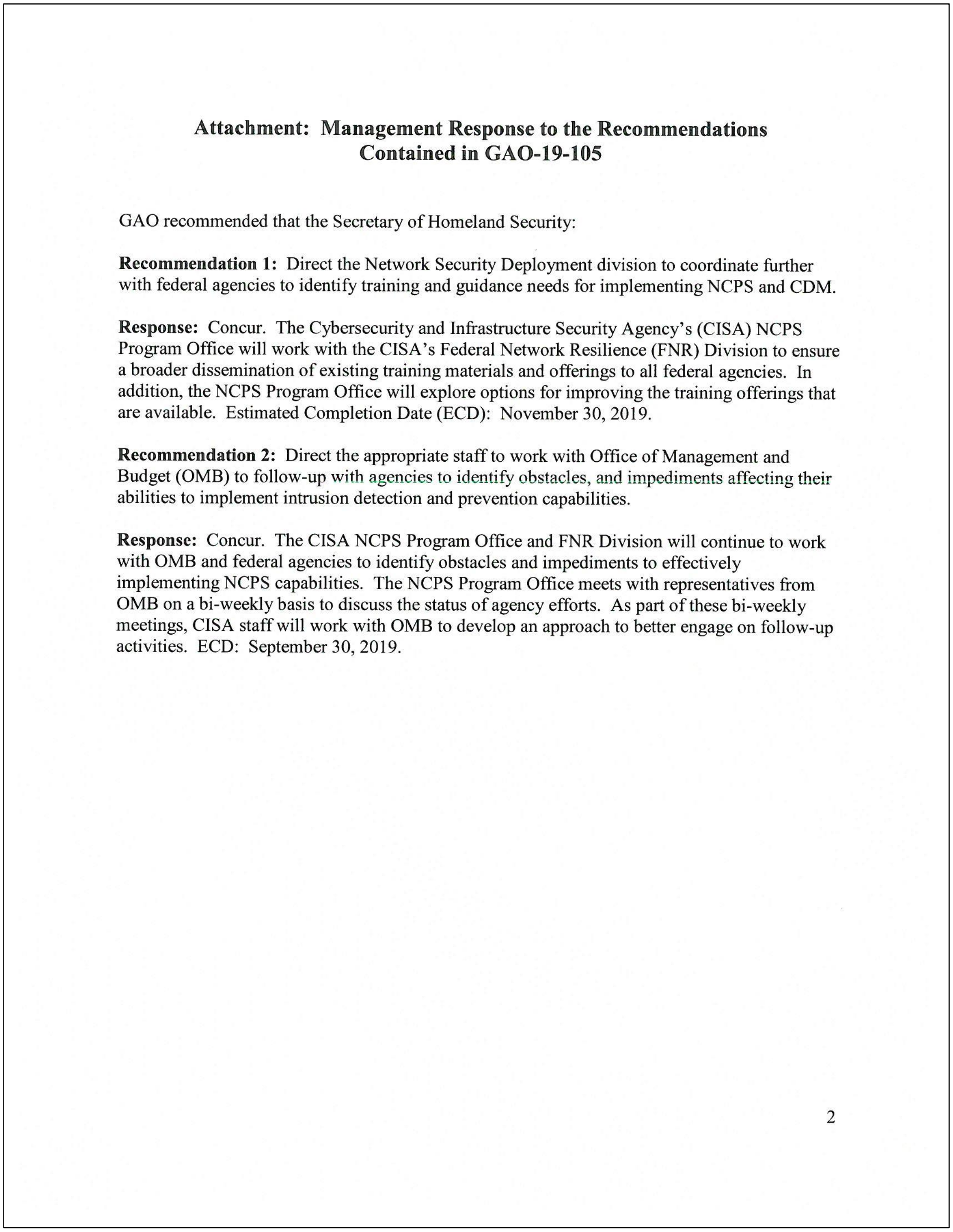
The draft report contained nine recommendations including two for DHS with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment



Attachment: Management Response to the Recommendations Contained in GAO-19-105

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct the Network Security Deployment division to coordinate further with federal agencies to identify training and guidance needs for implementing NCPS and CDM.

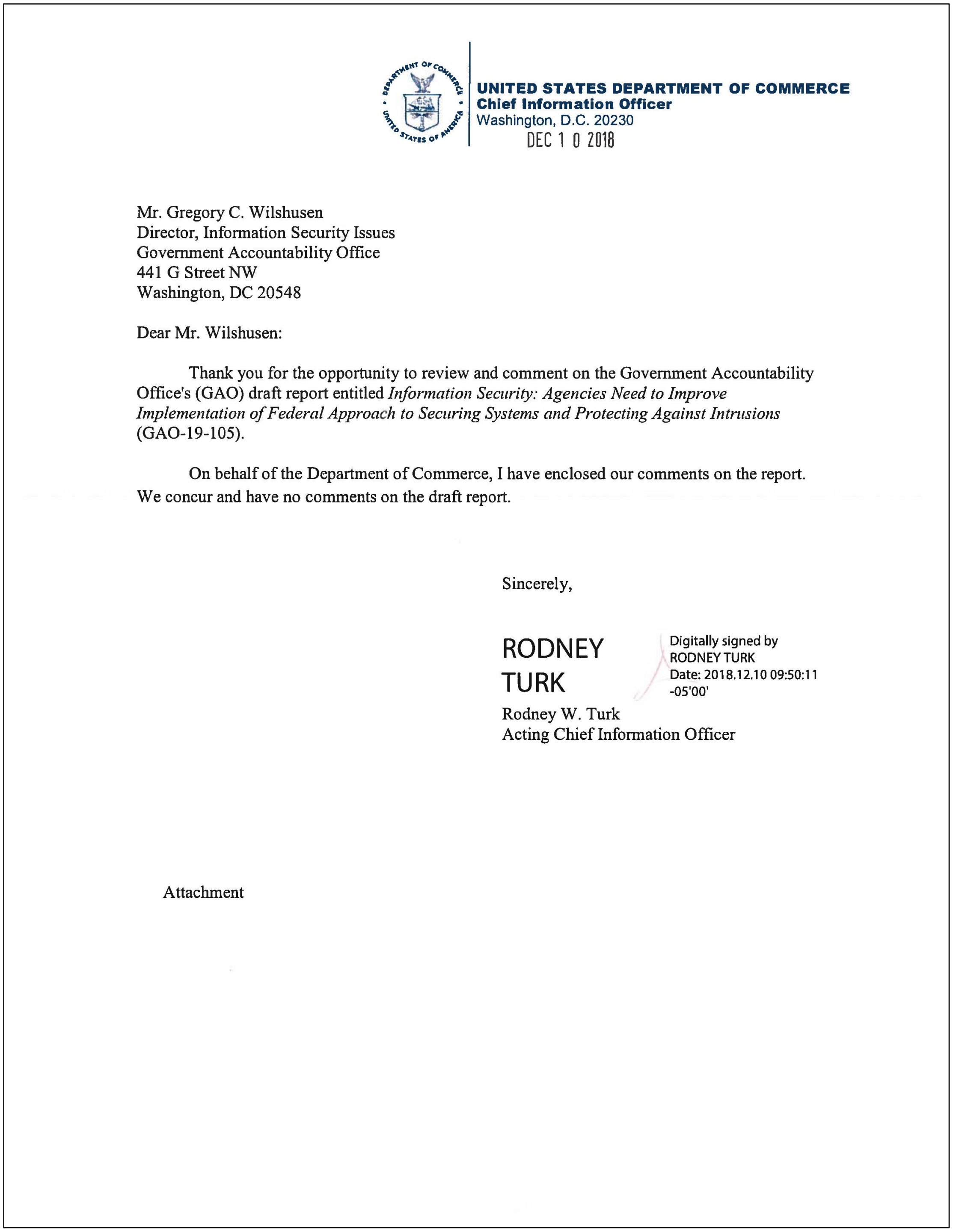
Response: Concur. The Cybersecurity and Infrastructure Security Agency's (CISA) NCPS Program Office will work with the CISA's Federal Network Resilience (FNR) Division to ensure a broader dissemination of existing training materials and offerings to all federal agencies. In addition, the NCPS Program Office will explore options for improving the training offerings that are available. Estimated Completion Date (ECD): November 30, 2019.

Recommendation 2: Direct the appropriate staff to work with Office of Management and Budget (OMB) to follow-up with agencies to identify obstacles, and impediments affecting their abilities to implement intrusion detection and prevention capabilities.

Response: Concur. The CISA NCPS Program Office and FNR Division will continue to work with OMB and federal agencies to identify obstacles and impediments to effectively implementing NCPS capabilities. The NCPS Program Office meets with representatives from OMB on a bi-weekly basis to discuss the status of agency efforts. As part of these bi-weekly meetings, CISA staff will work with OMB to develop an approach to better engage on follow-up activities. ECD: September 30, 2019.

Appendix VI: Comments from the Department of Commerce

Appendix VI: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

DEC 1 0 2018

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

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled *Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions* (GAO-19-105).

On behalf of the Department of Commerce, I have enclosed our comments on the report. We concur and have no comments on the draft report.

Sincerely,

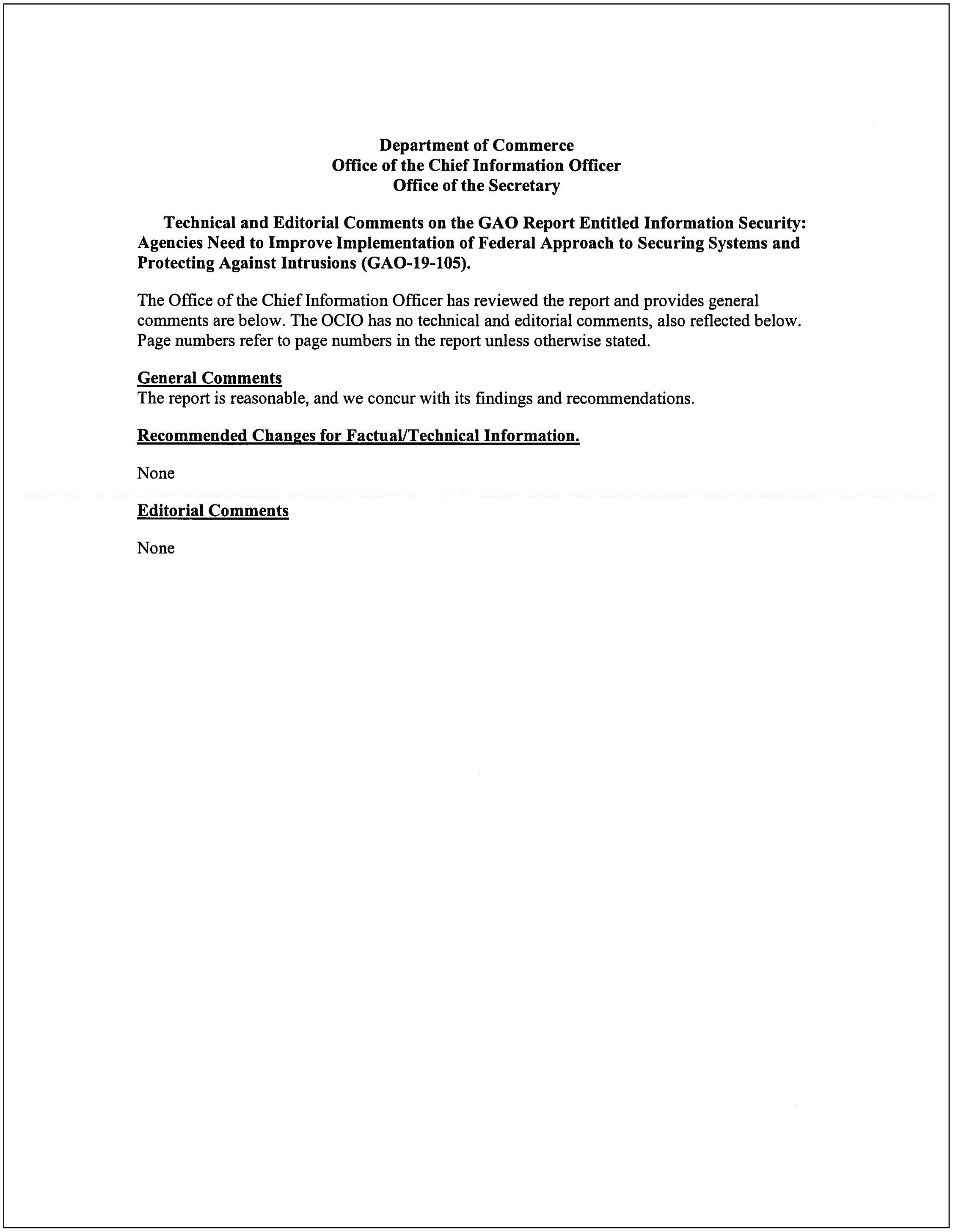
RODNEY TURK

Digitally signed by RODNEY TURK
Date: 2018.12.10 09:50:11 -05'00'

Rodney W. Turk
Acting Chief Information Officer

Attachment

Appendix VI: Comments from the Department of Commerce



Department of Commerce
Office of the Chief Information Officer
Office of the Secretary

Technical and Editorial Comments on the GAO Report Entitled Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions (GAO-19-105).

The Office of the Chief Information Officer has reviewed the report and provides general comments are below. The OCIO has no technical and editorial comments, also reflected below. Page numbers refer to page numbers in the report unless otherwise stated.

General Comments
The report is reasonable, and we concur with its findings and recommendations.

Recommended Changes for Factual/Technical Information.

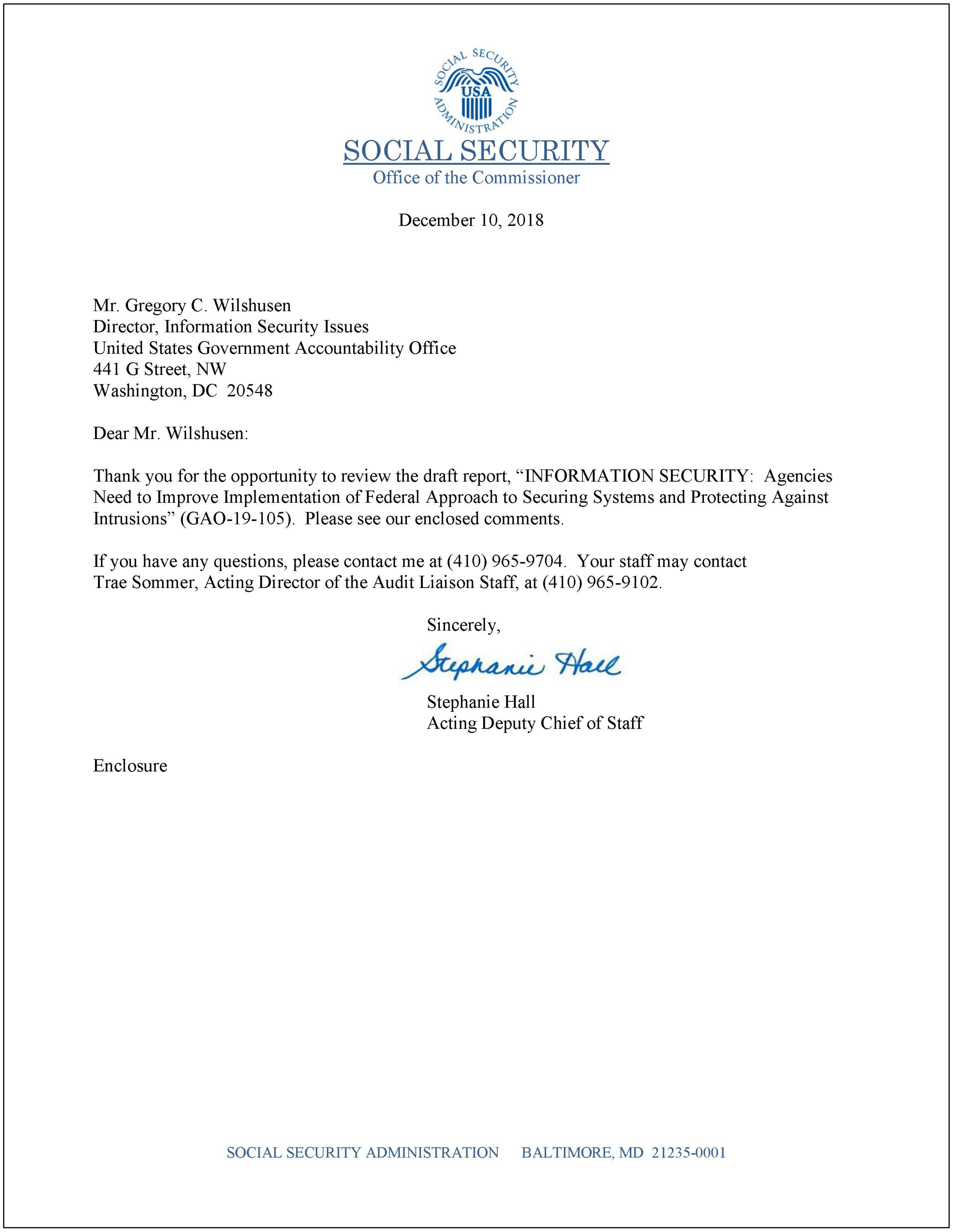
None

Editorial Comments

None

Appendix VII: Comments from the Social Security Administration

Appendix VII: Comments from the Social Security Administration



SOCIAL SECURITY

Office of the Commissioner

December 10, 2018

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, “INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions” (GAO-19-105). Please see our enclosed comments.

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.

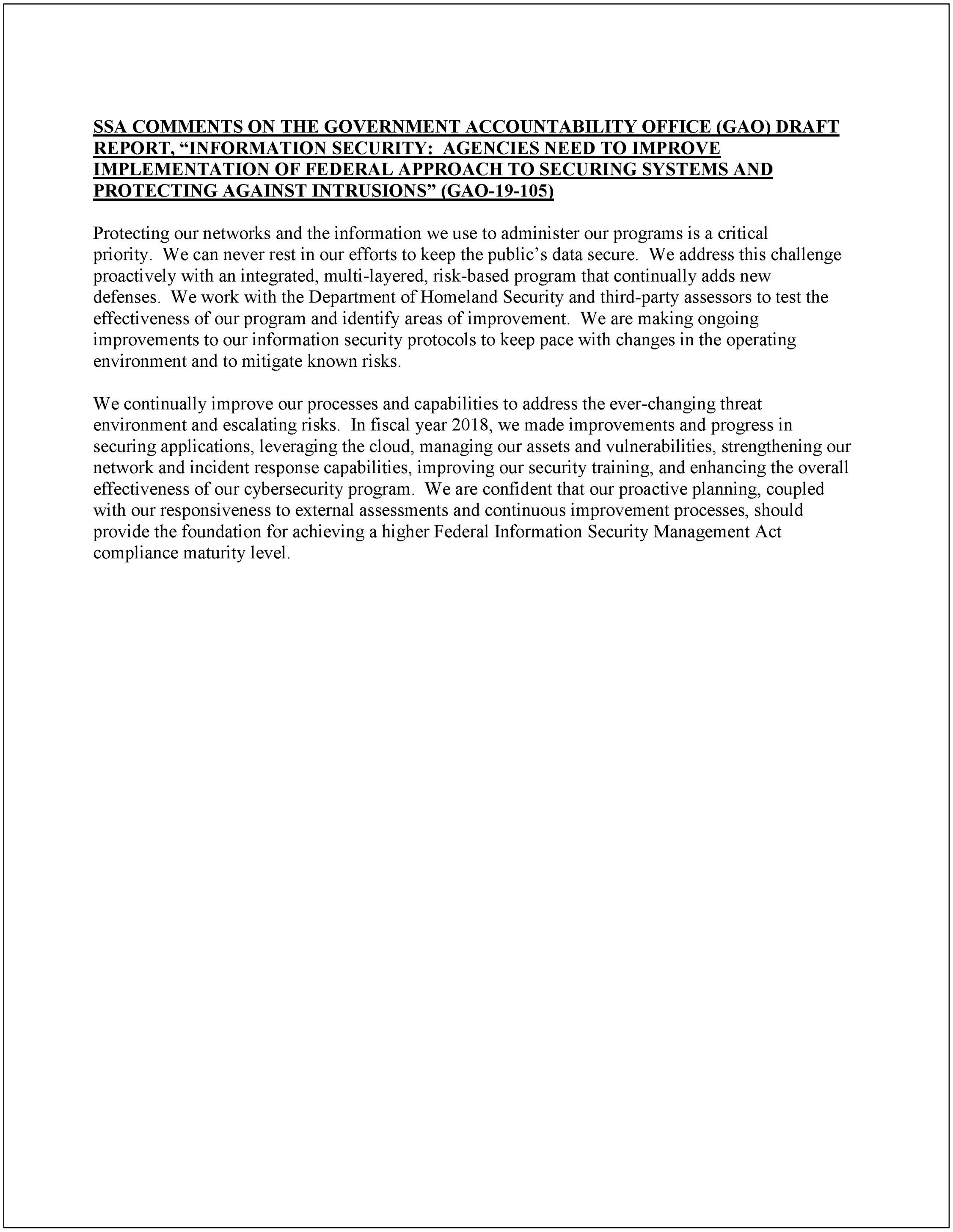
Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001



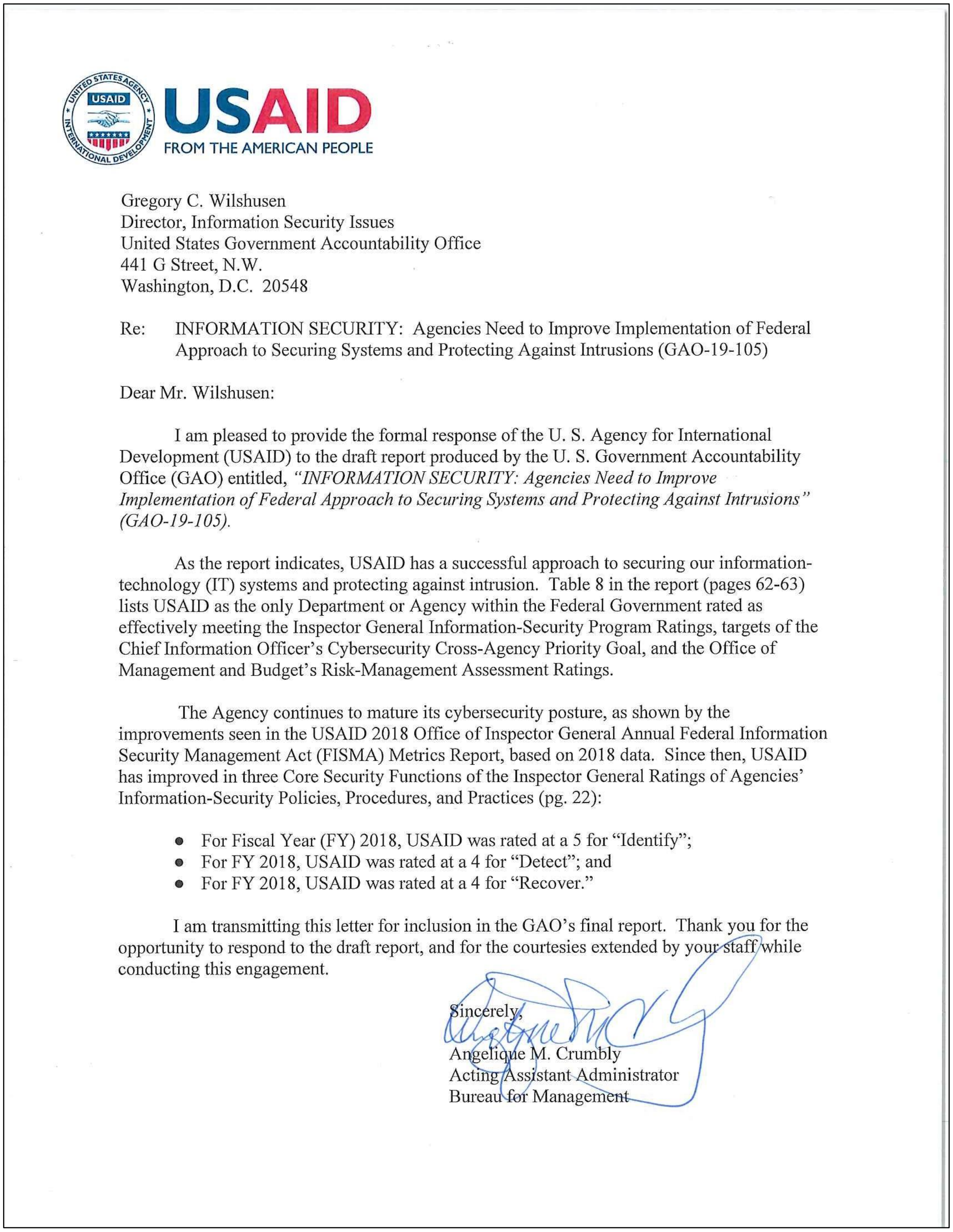
SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS" (GAO-19-105)

Protecting our networks and the information we use to administer our programs is a critical priority. We can never rest in our efforts to keep the public's data secure. We address this challenge proactively with an integrated, multi-layered, risk-based program that continually adds new defenses. We work with the Department of Homeland Security and third-party assessors to test the effectiveness of our program and identify areas of improvement. We are making ongoing improvements to our information security protocols to keep pace with changes in the operating environment and to mitigate known risks.

We continually improve our processes and capabilities to address the ever-changing threat environment and escalating risks. In fiscal year 2018, we made improvements and progress in securing applications, leveraging the cloud, managing our assets and vulnerabilities, strengthening our network and incident response capabilities, improving our security training, and enhancing the overall effectiveness of our cybersecurity program. We are confident that our proactive planning, coupled with our responsiveness to external assessments and continuous improvement processes, should provide the foundation for achieving a higher Federal Information Security Management Act compliance maturity level.

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

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



USAID
FROM THE AMERICAN PEOPLE

Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Re: INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions (GAO-19-105)

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) entitled, *"INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions" (GAO-19-105).*

As the report indicates, USAID has a successful approach to securing our information-technology (IT) systems and protecting against intrusion. Table 8 in the report (pages 62-63) lists USAID as the only Department or Agency within the Federal Government rated as effectively meeting the Inspector General Information-Security Program Ratings, targets of the Chief Information Officer's Cybersecurity Cross-Agency Priority Goal, and the Office of Management and Budget's Risk-Management Assessment Ratings.

The Agency continues to mature its cybersecurity posture, as shown by the improvements seen in the USAID 2018 Office of Inspector General Annual Federal Information Security Management Act (FISMA) Metrics Report, based on 2018 data. Since then, USAID has improved in three Core Security Functions of the Inspector General Ratings of Agencies' Information-Security Policies, Procedures, and Practices (pg. 22):

- For Fiscal Year (FY) 2018, USAID was rated at a 5 for "Identify";
- For FY 2018, USAID was rated at a 4 for "Detect"; and
- For FY 2018, USAID was rated at a 4 for "Recover."

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,

Angelique M. Crumbly
Acting Assistant Administrator
Bureau for Management

Appendix IX: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (assistant director), Daniel Swartz (analyst-in-charge), David Blanding, Chris Businsky, Kristi Dorsey, Di’Mond Spencer, Priscilla Smith, and Edward Varty made key contributions to this report. West Coile, Franklin Jackson, and Chris Warweg also provided assistance.

Appendix X: Accessible Data

Data Tables

Accessible Data for Risk Management Assessment Ratings by Core Security Function for the 23 Civilian Chief Financial Officers Act of 1990 Agencies, Fiscal Year 2017

Category	Level 1	level 2	level 3
Identify	9	10	4
Protect	10	11	2
Detect	19	4	0
Respond	12	11	0
Recover	15	8	0

Accessible Data for Figure 1: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2017

Other	Improper Usage	E-mail/ Phishing	Loss or Theft of Equipment	Web	Multiple Attack Vectors	Attrition	External/ Remov- able Media	Physical cause
10818	7856	7328	4395	4049	601	151	72	7

Accessible Data for Figure 3: Inspector General Ratings of Agencies' Information Security Policies, Procedures, and Practices Related to the Five Core Security Functions, as of Fiscal Year 2017

Category	Level 1	level 2	level 3	level 4	level 5
Recover	1	9	12	1	0
Respond	0	10	5	8	0
Detect	1	12	8	2	0
Protecta	0	8	10	4	0
Identity	1	7	11	4	0

Accessible Data for Figure 4: Number of Civilian Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Years 2016 and 2017

Category	FY 2016	FY 2017
Security management	11	12
Access control	19	17
Configuration management	16	16
Segregation of duties	7	9
Contingency planning	7	5

Accessible Data for Figure 5: Number of the 23 Selected Civilian Agencies That Reported Meeting Targets for the Cybersecurity Cross-Agency Priority Goal Priority Areas, Fiscal Years 2016 and 2017

Category	FY 2016	FY 2017
Information security continuous monitoring	6	8
Identity, credential, and access management	15	16
Anti-phishing and malware defense	14	17

Accessible Data for Figure 6: Risk Management Assessment Ratings by Core Security Function for the 23 Civilian Chief Financial Officers Act of 1990 Agencies, Fiscal Year 2017

Category	Level 1	level 2	level 3
Identify	9	10	4
Protect	10	11	2
Detect	19	4	0
Respond	12	11	0
Recover	15	8	0

Accessible Data for Figure 7: Civilian Chief Financial Officers Act of 1990 Agencies' Implementation of DHS's Continuous Diagnostics and Mitigation Program Phases, as of June 2018

Phase	Implemented	Partially Implemented	Not Implemented at all
Phase 1	8	15	0
Phase 2	2	17	4
Phase 3	0	4	19

Agency Comment Letters

Accessible Text for Appendix V Comments from the Department of Homeland Security

Page 1

December 11, 2018

Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-19-105, "INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions" (Job Code 102490)

Dear Mr. Wilshusen,

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of DHS initiatives being taken to further secure agency information systems. These include the development of an in-depth "Intrusion Assessment Plan" that outlines tools, platforms, and resources; development of the National Cybersecurity Protection System (NCPS); and providing tools and services to agencies to monitor their networks through the Continuous Diagnostic and Mitigation (CDM) program. DHS is committed to helping agencies, which are responsible for their own cybersecurity, reduce the risk of successful cyber-attacks.

The draft report contained nine recommendations including two for DHS with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 2

Attachment: Management Response to the Recommendations Contained in GAO-19-105

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Direct the Network Security Deployment division to coordinate further with federal agencies to identify training and guidance needs for implementing NCPS and COM.

Response: Concur. The Cybersecurity and Infrastructure Security Agency's (CISA) NCPS Program Office will work with the CISA's Federal Network Resilience (FNR) Division to ensure a broader dissemination of existing training materials and offerings to all federal agencies. In addition, the NCPS Program Office will explore options for improving the training offerings that are available. Estimated Completion Date (ECO): November 30, 2019.

Recommendation 2: Direct the appropriate staff to work with Office of Management and Budget (OMB) to follow-up with agencies to identify obstacles, and impediments affecting their abilities to implement intrusion detection and prevention capabilities.

Response: Concur. The CISA NCPS Program Office and FNR Division will continue to work with 0MB and federal agencies to identify obstacles and impediments to effectively implementing NCPS capabilities. The NCPS Program Office meets with representatives from 0MB on a bi-weekly basis to discuss the status of agency efforts. As part of these bi-weekly meetings, CISA staff will work with 0MB to develop an approach to better engage on follow-up activities. ECO: September 30, 2019.

Accessible Text for Appendix VI Comments from the Department of Commerce

Page 1

DEC 10 2018

Mr. Gregory C. Wilshusen

Director, Information Security Issues

Government Accountability Office

441 G Street NW

Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report entitled Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions (GAO-19-105).

On behalf of the Department of Commerce, I have enclosed our comments on the report. We concur and have no comments on the draft report.

Sincerely,

Rodney W. Turk

Acting Chief Information Officer

Attachment

Page 2

Department of Commerce

Office of the Chief Information Officer

Office of the Secretary

Technical and Editorial Comments on the GAO Report Entitled Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions (GAO-19-105).

The Office of the Chief Information Officer has reviewed the report and provides general comments are below. The OCIO has no technical and editorial comments, also reflected below. Page numbers refer to page numbers in the report unless otherwise stated.

General Comments

The report is reasonable, and we concur with its findings and recommendations.

Recommended Changes for Factual/Technical Information.

None

Editorial Comments

None

Accessible Text for Appendix VII Comments from the Social Security Administration

Page 1

December 10, 2018

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, “INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions” (GAO-19-105). Please see our enclosed comments.

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

Enclosure

Page 2

SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, “INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO

SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS" (GAO-19-105)

Protecting our networks and the information we use to administer our programs is a critical priority. We can never rest in our efforts to keep the public's data secure. We address this challenge proactively with an integrated, multi-layered, risk-based program that continually adds new defenses. We work with the Department of Homeland Security and third-party assessors to test the effectiveness of our program and identify areas of improvement. We are making ongoing improvements to our information security protocols to keep pace with changes in the operating environment and to mitigate known risks.

We continually improve our processes and capabilities to address the ever-changing threat environment and escalating risks. In fiscal year 2018, we made improvements and progress in securing applications, leveraging the cloud, managing our assets and vulnerabilities, strengthening our network and incident response capabilities, improving our security training, and enhancing the overall effectiveness of our cybersecurity program. We are confident that our proactive planning, coupled with our responsiveness to external assessments and continuous improvement processes, should provide the foundation for achieving a higher Federal Information Security Management Act compliance maturity level.

Accessible Text for Appendix VIII Comments from the U.S. Agency for International Development

Gregory C. Wilshusen

Director, Information Security Issues

United States Government Accountability Office

441 G Street, N.W.

Washington, D.C. 20548

Re: INFORMATION SECURITY: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions (GAO-19-105)

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) entitled, “INFORMATION SECURITY• Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions” (GAO-19-105).

As the report indicates, USAID has a successful approach to securing our information- technology (IT) systems and protecting against intrusion. Table 8 in the report (pages 62-63) lists USAID as the only Department or Agency within the Federal Government rated as effectively meeting the Inspector General Information-Security Program Ratings, targets of the Chief Information Officer's Cybersecurity Cross-Agency Priority Goal, and the Office of Management and Budget's Risk-Management Assessment Ratings.

The Agency continues to mature its cybersecurity posture, as shown by the improvements seen in the USAID 2018 Office of Inspector General Annual Federal Information Security Management Act (FISMA) Metrics Report, based on 2018 data. Since then, USAID has improved in three Core Security Functions of the Inspector General Ratings of Agencies' Information-Security Policies, Procedures, and Practices (pg. 22):

- For Fiscal Year (FY) 2018, USAID was rated at a 5 for "Identify";
- For FY 2018, USAID was rated at a 4 for "Detect"; and
- For FY 2018, USAID was rated at a 4 for "Recover."

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,

Angelique M. Crumbly

Acting Assistant Administrator

Bureau for Management

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:

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