United States Government Accountability Office

Report to Congressional Committees

March 2022

# CYBERSECURITY

# OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision

# GAO Highlights

Highlights of GAO-22-104364, a report to congressional committees

March 2022

# CYBERSECURITY

## OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision

## Why GAO Did This Study

Since 1997, GAO has designated information security as a government-wide high-risk area. To protect federal information and systems, FISMA requires federal agencies to develop, document, and implement information security programs. Congress included a provision in FISMA for GAO to periodically report on agencies' implementation of the act.

GAO's objectives in this report were to (1) describe the reported effectiveness of federal agencies' implementation of cybersecurity policies and practices and (2) evaluate the extent to which relevant officials at federal agencies consider FISMA to be effective at improving the security of agency information systems.

To do so, GAO reviewed the 23 civilian CFO Act agencies' FISMA reports, agency reported performance data, past GAO reports, and OMB documentation and guidance. GAO also interviewed agency officials from the 24 CFO Act agencies (i.e., the 23 civilian CFO Act agencies and the Department of Defense), the Council of IGs on Integrity and Efficiency, and OMB.

## What GAO Recommends

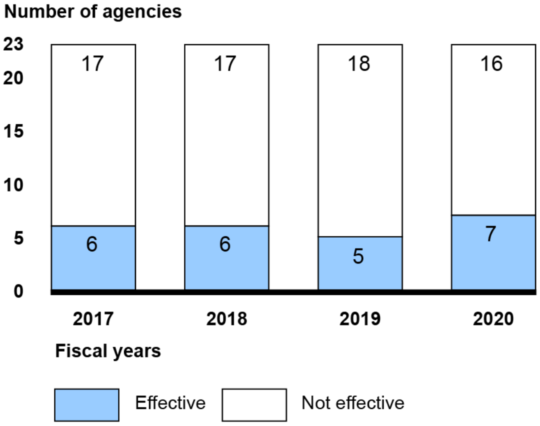
GAO is making two recommendations that OMB, in consultation with others, clarify its guidance to IGs and create a more precise overall rating scale. OMB did not concur with our recommendations, stating, in part, that they want to provide IGs with the flexibility to adapt their reviews. Nevertheless, GAO believes that the recommendations are warranted in order to provide a more consistent and accurate picture of agencies' cybersecurity performance.

View GAO-22-104364. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

## What GAO Found

In fiscal year 2020, the effectiveness of federal agencies' implementation of requirements set by the *Federal Information Security Modernization Act of 2014* (FISMA) was mixed. For example, more agencies reported meeting goals for managing the security of their software assets, as well as for intrusion detection and prevention. Nevertheless, inspectors general (IG) identified agencies' uneven performance of cybersecurity practices. For fiscal year 2020, IGs determined that seven of the 23 civilian *Chief Financial Officers* (CFO) *Act of 1990* agencies had effective information security programs. Between fiscal years 2017 and 2020, the percentage of agencies receiving effective ratings has generally been consistent, ranging from 22 to 30 percent.

**Number of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies with Effective and Not Effective Agency-Wide Information Security Programs, as Reported by Inspectors General for Fiscal Years 2017-2020**



Source: GAO analysis of inspector general report data and Office of Management and Budget's *Federal Information Security Modernization Act of 2014* reports to Congress. | GAO-22-104364

According to officials at all 24 CFO Act agencies, FISMA and its associated reporting process enabled their agencies to improve their information security programs' effectiveness. Specifically, Chief Information Officers and Chief Information Security Officers at 14 agencies stated that FISMA improved program effectiveness to a great extent, while officials at 10 agencies said it improved effectiveness to a moderate extent.

As required under FISMA, the Office of Management and Budget (OMB), in partnership with other organizations, provides guidance to IGs on conducting and reporting agency FISMA evaluations. GAO found that this guidance was not always clear, leading to inconsistent application by IGs. Further, GAO found that OMB's overall IG rating scale of "effective" and "not effective" resulted in imprecise ratings that did not clearly distinguish the differing levels of agencies' implementation of cybersecurity requirements. As a result, IG ratings may be less useful for cybersecurity oversight. By clarifying its future ratings guidance and improving its rating scale, OMB could help ensure that the reviews provide a more consistent picture of agencies' cybersecurity performance, enabling Congress to better understand agencies' relative cybersecurity risks.

# Contents

Tables

Figures

## Abbreviations

| | |
|---|---|
| AAL3 | authenticator assurance level 3 |
| CAP | Cross-Agency Priority |
| CDC | Centers for Disease Control and Prevention |
| CDM | Continuous Diagnostics and Mitigation |
| CFO | Chief Financial Officer |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| CIO | Chief Information Officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| DHS | Department of Homeland Security |
| DMDC | Defense Manpower Data Center |
| DOD | Department of Defense |
| EPA | Environmental Protection Agency |
| FedRAMP | Federal Risk and Authorization Management Program |
| FISMA | Federal Information Security Modernization Act of 2014 |
| GSA | General Services Administration |
| HHS | Department of Health and Human Services |
| HUD | Department of Housing and Urban Development |
| IG | Inspector General |
| NIST | National Institute of Standards and Technology |
| NRC | Nuclear Regulatory Commission |
| NSF | National Science Foundation |
| OMB | Office of Management and Budget |
| PII | personally identifiable information |
| PIV | personal identity verification |
| SSA | Social Security Administration |
| US-CERT | United States Computer Emergency Readiness Team |
| USAID | U.S. Agency for International Development |
| VA | Department of Veterans Affairs |

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

March 31, 2022

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

The security of federal IT systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of government operations and assets.

In May 2021, the Office of Management and Budget (OMB) reported an increased number of cybersecurity incidents at federal agencies, stating that this increase highlights the ever-expanding threats within the digital landscape and the need for the federal government to take action to reduce the impact of cybersecurity incidents. Although not addressed in OMB's May 2021 report, the SolarWinds Orion incident is a recent example of a breach that resulted in a number of federal agencies receiving software updates that had been compromised with malicious code.[1] This incident and others show that federal information systems continue to remain at risk from cybersecurity threats.

GAO first designated information security as a government-wide high-risk area in 1997.[2] In September 2018 and again in March 2021, our high-risk reports emphasized the need for the federal government to take actions

[1] SolarWinds Orion is a network management and monitoring suite of software products.

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

to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[3] Most recently, we continued to identify federal information security as a government-wide high-risk area in our March 2021 high-risk update.[4]

From 2010 through January 2022, we made approximately 3,800 recommendations focused on enhancing our nation's cybersecurity efforts. Among other things, these recommendations identified actions agencies should take to strengthen their information security programs. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part, because they have not implemented many of these recommendations. As of January 2022, approximately 880 of the 3,800 cybersecurity recommendations had not been implemented.

The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program to protect the information and systems that support the agencies' operations and assets.[5] The act also requires agencies to submit Chief Information Officer (CIO) FISMA reports on their agency's cybersecurity. These reports are to include the metrics that agencies use to assess their progress toward outcomes intended to strengthen federal cybersecurity. In addition to the CIO FISMA reports, the act requires each agency's Inspector General (IG) or independent external auditor to perform an annual independent

[3] See GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021) and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[4] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[5] The *Federal Information Security Modernization Act of 2014* (FISMA 2014), 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 to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

evaluation to determine and report on the effectiveness of its agency's information security program.

FISMA includes a provision for GAO to periodically report to Congress on agencies' implementation of the act. Our specific objectives for this report were to (1) describe the reported effectiveness of federal agencies' implementation of cybersecurity policies and practices and (2) evaluate the extent to which relevant officials at federal agencies consider FISMA to be effective at improving the security of agency information systems.

To address the first objective, we analyzed the 23 civilian *Chief Financial Officers* (CFO) *Act of 1990* agencies' reported progress toward implementing government-wide cybersecurity targets for fiscal years 2018 through 2020; OMB's annual FISMA reports to Congress for fiscal years 2017 through 2020; and the annual FISMA assessments issued by the 23 agencies' IGs for fiscal years 2017 through 2020.[6] We also reviewed our

[6] The 24 agencies covered by the CFO Act of 1990, 31 U.S.C. § 901(b) are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Office of Personnel Management, the Small Business Administration, the Social Security Administration, and the U.S. Agency for International Development. The civilian CFO Act agencies include all of the aforementioned agencies except for the Department of Defense (DOD). We did not include DOD in our analysis of agencies' performance data because the data were not publicly available. Further, we did not include DOD in our analysis of the fiscal year 2017-2020 FISMA reports due to concerns with data sensitivity.

reports on federal cybersecurity, issued from October 2018 through May 2021.[7]

We summarized performance data outlining agencies' reported progress toward implementing federal cybersecurity targets supporting the cybersecurity-related initiative in the IT Modernization Cross Agency Priority (CAP) goal.[8] To do so, we first obtained publicly available performance data that showed the 23 agencies' reported status against the CAP goal targets at the end of fiscal year 2020.[9] We also used these

[7] The reports that we selected for this review were: GAO, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls,* GAO-21-401R (Washington, D.C.: May 4, 2021); *Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment,* GAO-20-252 (Washington, D.C.: Sept. 30, 2020); *Information Security and Privacy: HUD Needs a Major Effort to Protect Data Shared with External Entities,* GAO-20-431 (Washington, D.C.: Sept. 21, 2020); *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program,* GAO-20-598 (Washington, D.C.: Aug. 18, 2020); *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene,* GAO-20-241 (Washington, D.C.: Apr. 13, 2020); *Information Technology: DHS Directives Have Strengthened Federal Cybersecurity, but Improvements Are Needed,* GAO-20-133 (Washington, D.C.: Feb. 4, 2020); *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed,* GAO-20-126 (Washington, D.C.: Dec. 12, 2019); *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges,* GAO-19-384 (Washington, D.C.: July 25, 2019); and *Information Security: Significant Progress Made, but CDC Needs to Take Further Action to Resolve Control Deficiencies and Improve Its Program,* GAO-19-70 (Washington, D.C.: Dec. 20, 2018).

[8] The CAP goals are 4-year outcome-oriented goals that measure federal progress toward implementing the President's Management Agenda. The previous administration's President's Management Agenda was 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. One of the CAP goals, IT Modernization, contained a cybersecurity initiative. The initiative was designed to reduce cybersecurity risks to the federal government's information systems by mitigating the impact of risks to federal data, systems, and networks. The initiative consisted of three strategies that contained cybersecurity-related targets. The current administration issued the *Biden-Harris Management Agenda Vision* in November 2021, but specific targets and CAP goals associated with the agenda have not yet been released as of March 15, 2022.

[9] OMB and General Services Administration (GSA) published the 23 civilian CFO Act agencies' reported fiscal year 2020 CAP goal data. See General Services Administration and Office of Management and Budget, *Performance.gov/data (Beta): Visualizing Agency and Performance Data*, (Washington, D.C.) accessed September 2021, https://trumpadministration.archives.performance.gov/data/. As stated in footnote 6, we did not include DOD in our analysis of agencies' performance against the cybersecurity-related CAP goal targets because DOD was not included in the publicly available CAP goal performance data at these websites.

data to determine which agencies met the CAP goal's cybersecurity-related targets at the end of fiscal year 2020. We compared the fiscal year 2020 CAP goal data to reported CAP goal data for fiscal years 2018 and 2019 to show the agencies' progress over time.

Further, we analyzed the annual OMB FISMA reports to Congress and the IG FISMA reports for fiscal years 2017 through 2020 for each of the 23 agencies. We then relied on the analysis to develop an overview of the state of federal cybersecurity and a summary of government-wide FISMA implementation. We also used the FISMA reports to summarize the IGs' overall information security program ratings for fiscal years 2017 to 2020.

In addition, we reviewed the IGs' fiscal year 2020 maturity level ratings for their agencies in each of the five core security functions identified in the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.[10] Further, we compared the fiscal year 2020 IG FISMA maturity level ratings to those from fiscal year 2019 to determine how the evaluations changed. We asked relevant agency and IG officials for additional information to account for changes in their agencies' maturity ratings between fiscal years 2019 and 2020. If applicable, we also asked relevant agency and IG officials to explain the rationale for rating any core security function at the lowest possible maturity level, Level 1 (Ad Hoc), for fiscal year 2020.

As part of our analyses, we assessed the reliability of the data sources by checking for any obvious issues or incomplete or missing data and by interviewing knowledgeable agency officials. Based on our assessment of this information, we concluded that the data and our sources were sufficiently reliable for the purposes of describing the reported

[10] Agency IGs are to assign a maturity level rating for each of the five Cybersecurity Framework core security functions based on an assessment of their agencies' implementation of the activities and controls associated with each function. The Cybersecurity Framework's core security functions represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in expressing their management of cybersecurity risk at a high level and enabling risk management decisions. The maturity ratings are on a five-level scale, with each succeeding level representing a more advanced level of the function's implementation. See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (Gaithersburg, MD: Apr. 16, 2018); and *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1* (May 2021).

effectiveness of federal agencies' implementation of cybersecurity policies and practices.

In addition, we reviewed GAO reports on government-wide cybersecurity initiatives and individual agencies' IT security programs, issued from October 2018 through May 2021, and summarized our findings related to the effectiveness of federal agencies' information security policies and practices. We included only reports that focused on federal agencies' cybersecurity programs. We excluded those reports that related to critical infrastructure protection and those that were classified or marked as sensitive.[11] We then used our professional judgment to determine whether the remaining reports were related to FISMA requirements or FISMA report metrics and audited at least one CFO Act agency.[12] If we found that the reports met either threshold, we included them in our review.

To address the second objective, we evaluated the extent to which relevant officials at federal agencies considered FISMA to be effective at improving the security of agency information systems. To do so, we conducted structured interviews with CIOs and Chief Information Security Officers (CISO) at the 24 CFO Act agencies (i.e., the 23 civilian CFO Act agencies and DOD). We focused our interviews and subsequent analysis around three areas of inquiry: (1) how, if at all, officials thought FISMA had helped to improve the effectiveness of agencies' information security programs; (2) whether the officials perceived any impediments to their agencies' implementation of FISMA; and (3) whether the officials had any suggested changes to improve FISMA or the FISMA reporting process. For consistency across the interviews, we asked the agency officials a list of identical multiple-choice and open-ended questions.

We then reviewed the agency officials' responses and compared them to our structured interview questions to determine the most commonly cited responses for each of the aforementioned areas of inquiry. Specifically,

[11] The term "critical infrastructure" refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. [See 42 U.S.C. §5195c(e).] Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[12] We also considered GAO reports that reviewed components of the 24 CFO Act agencies.

for the multiple-choice questions, we compiled the agencies' answers to determine the frequency of each choice. To analyze narrative questions, we sorted similar responses into categories and then determined which categories were the most frequently cited. At the end of each step of the process, another GAO analyst validated the determinations to help ensure consistency in the categorization of each agency's responses.

In addition, we interviewed officials representing organizations with operational and oversight responsibilities for cybersecurity across the federal government. Specifically, we interviewed officials at the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), OMB, and the Council of IGs on Integrity and Efficiency's (CIGIE) Technology Committee to elicit their views on the agency officials' comments and suggestions.[13] To assess the sufficiency of their suggestions, we compared the responses from these officials to OMB's guidance and the FISMA performance metrics.

We conducted this performance audit from June 2020 to March 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

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

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their

[13] In addition to our interview, CIGIE's Technology Committee surveyed its members to provide additional IG perspectives. The IG respondents represented 16 diverse federal organizations: eight CFO Act agencies, four independent agencies, and four members of the intelligence community. The CIGIE officials did not specify which specific agencies responded to their survey in order to maintain the IGs' anonymity.

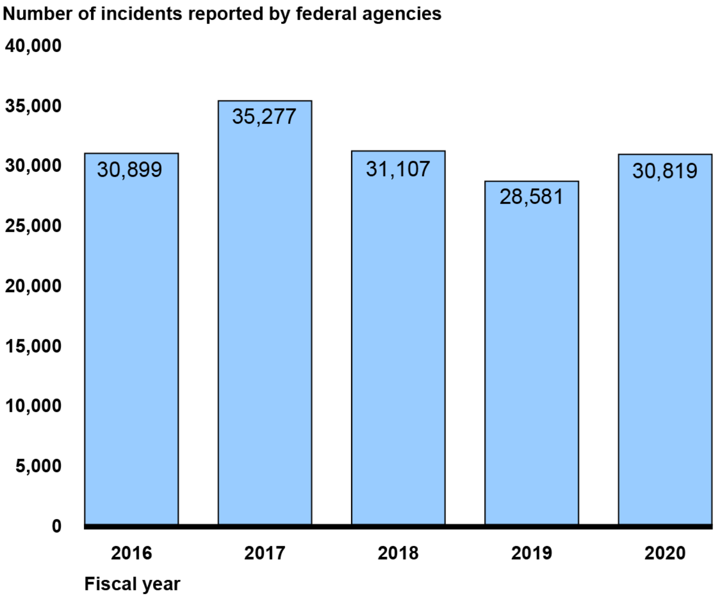
access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Cyber-based threats to information systems can come from sources internal and external to the organization. Internal threats include errors or mistakes, as well as fraudulent or malevolent acts by employees or contractors working within the organization. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as individuals, groups, and countries that wish to do harm to an organization's systems.

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

## Number of Reported Incidents Showed Little Change from Fiscal Years 2016 to 2020

FISMA requires agencies across the government, including both CFO Act and non-CFO Act agencies, to report their cybersecurity incidents to the United States Computer Emergency Readiness Team (US-CERT), a component of DHS. As illustrated in figure 1, the US-CERT and OMB incident report data show that agencies reported an average of approximately 31,337 incidents per year between fiscal years 2016 and 2020. Agencies reported 30,819 incidents in fiscal year 2020—2,238 incidents higher than reported in fiscal year 2019, but the overall 5-year trend in number of incidents showed little change.

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2016 through 2020

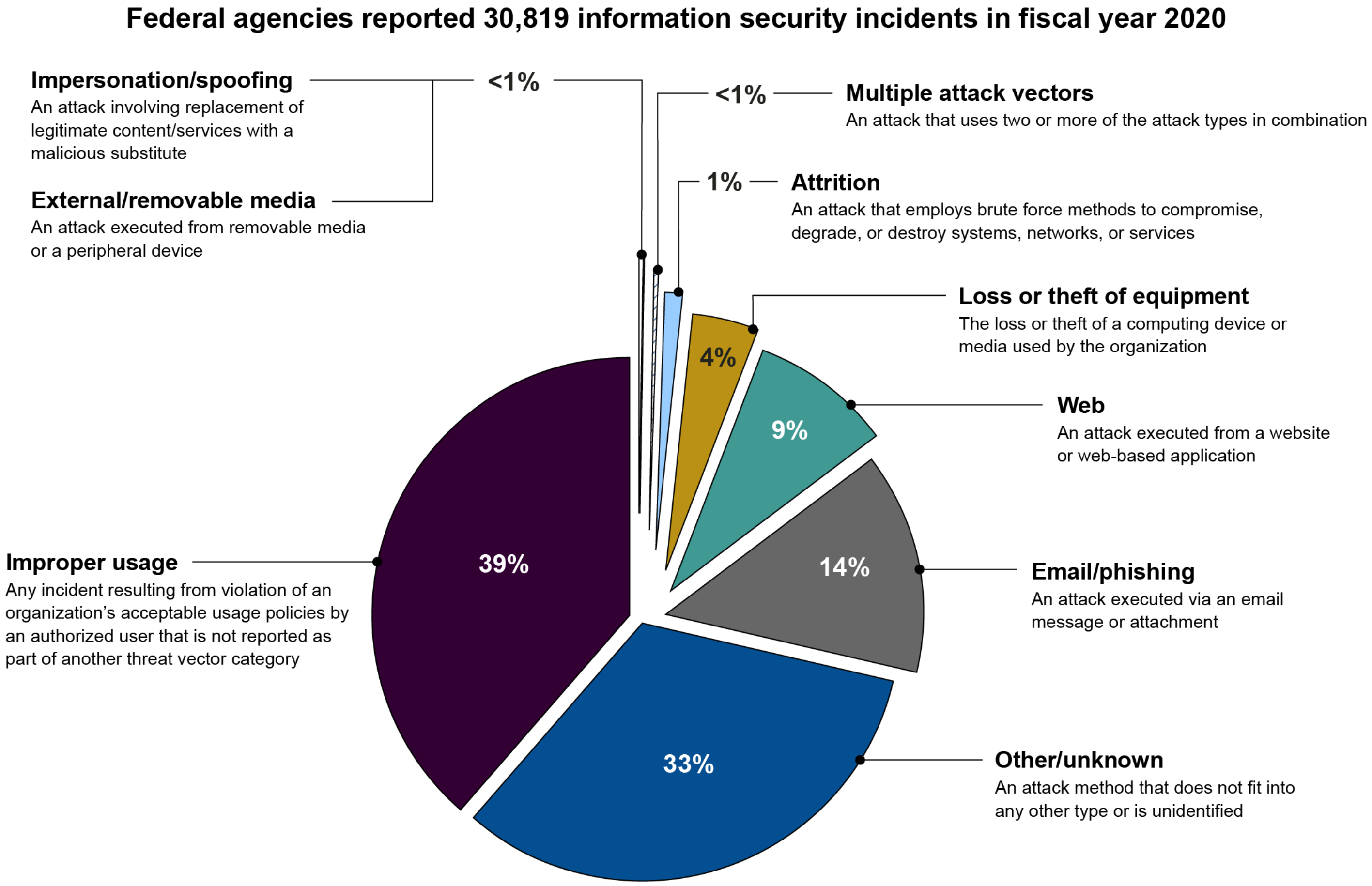


Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data. | GAO-22-104364

According to US-CERT incident report data, the incidents reported in fiscal year 2020 involved several threat vectors, including web-based attacks, phishing attacks, and the loss or theft of computer equipment, among others.[14] Figure 2 provides a breakdown of the fiscal year 2020 information security incidents by threat vector.

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

**Figure 2: Information Security Incidents Reported by Federal Agencies and Categorized by Threat Vector in Fiscal Year 2020**



Source: United States Computer Emergency Readiness Team incident report data for fiscal year 2020. | GAO-22-104364

According to OMB's annual FISMA report to Congress, the prevalence of the "Improper usage" vector indicates that agencies have processes or capabilities that detect when a security policy is being violated, but lack automated enforcement or prevention mechanisms. The OMB report also stated that the prevalence of the "Other/unknown" attack vector suggests additional steps should be taken to ensure agencies appropriately categorize the vector of incidents during reporting. OMB noted that it and CISA will work with agencies to ensure that the vectors of incidents are appropriately categorized.

FISMA also requires agencies to report and provide a description of any major security incident that occurs.[15] Major incidents can pose a serious threat to national security and public safety. Each year, major security incidents reported by agencies are summarized in OMB's annual FISMA report to Congress. In its fiscal year 2020 report to Congress, OMB summarized the following six major incidents along with the agencies' subsequent responses and mitigations:[16]

- In September 2020, DOD reported a major incident at the Defense Manpower Data Center (DMDC) in which a data analyst mistakenly sent an incorrect dataset to a Navy civilian employee through the DMDC Request System, a secure file transfer application. The dataset included personal information, including names, Social Security numbers, dates of birth, home addresses, personnel information, gender, and race. Upon receipt of the dataset, the Navy employee notified DOD of the error and deleted the downloaded information. DOD took actions in response to this incident. For example, the personnel in the team that sent the incorrect information received supplementary training covering the importance of appropriate handling of personally identifiable information (PII). An estimated 300,000 individuals were potentially affected.
- In July 2020, the Department of Education reported a major incident in which a shared drive was open and accessible to users within the department. This shared drive included sensitive files containing the PII of student loan recipients. In response to this incident, the department restored proper file permissions to only those employees who required access to the information. The department found no evidence of improper use or unauthorized external disclosure of the PII. An estimated 304,668 individuals were potentially affected.
- In March 2020, DHS reported that a system storing PII had used substandard access controls when transmitting and storing data since 2007. Of the six vendors with contracts to access the system, only

[15] As defined by OMB, a major incident is either: (1) any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people or (2) a breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

[16] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2020* (Washington, D.C.: May 21, 2021).

one vendor had applicable cybersecurity and privacy clauses for proper system access. A third party's analysis found no evidence of a breach and did not detect any PII on the vendor-owned systems. An estimated 2.5 million individuals were potentially affected.

- In February 2020, DHS reported a major incident involving the improper storage, processing, and transfer of PII that included names, addresses, telephone numbers, and professional license numbers to an unaccredited server. A third-party assessor determined that the unaccredited systems showed no indication of compromise. DHS undertook remediation activities such as putting restrictions on external data transfers and modifying vendor contracts in order for the server to comply with cybersecurity and data sharing policies. An estimated 6.8 million individuals were potentially affected.
- In January 2020, the Department of Justice reported a major incident in which personal information, including names, addresses, birth dates, Social Security numbers, and alien numbers of current and former prisoners was stolen. In response to this incident, Justice changed the firewall rules for the affected system, made improvements to logging and detection systems, and required the revalidation of user accounts, among other actions. An estimated 387,000 individuals were potentially affected.
- In October 2019, DHS reported a major incident in which PII—including full names, home addresses, phone numbers, e-mail addresses—and several other non-PII elements were erroneously sent to a vendor. The vendor certified the destruction of all of the shared email addresses. An estimated 307,000 individuals were potentially affected.

Another major incident that affected multiple federal agencies was the cybersecurity breach of the SolarWinds Orion software. According to OMB, this breach was not included in OMB's fiscal year 2020 annual report to Congress because it was initially reported in December 2020, which was in fiscal year 2021.[17] The breach of the SolarWinds Orion software was one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector and affected agencies such as the Departments of Justice and Energy.

[17] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2020* (Washington, D.C.: May 21, 2021).

As we previously reported, beginning in September 2019, a campaign of cyberattacks by a foreign threat actor breached the computing networks at SolarWinds—a network management software company.[18] In February 2020, the threat actor began injecting hidden code into a file that was later included in the SolarWinds Orion software updates. SolarWinds released the software updates to its customers not realizing that the updates were compromised. The hidden code provided the threat actor with a "backdoor"—a program that can give an intruder remote access to an infected computer.

We also reported that, since SolarWinds Orion was widely used in the federal government to monitor network activity on federal systems, this incident allowed the threat actor to breach infected agency information systems. SolarWinds estimated that nearly 18,000 of its customers received a compromised software update. Of those, the threat actor targeted a smaller subset of high-value customers, including the federal government, to exploit for the primary purpose of espionage.

According to OMB, the SolarWinds Orion breach is expected to be a part of the fiscal year 2021 incident reporting included in the annual report to Congress. We also released a comprehensive review of this breach in January 2022.[19]

## FISMA Established Requirements for Effectively Securing Federal Information and Systems

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

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

[18] GAO, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021), accessed August 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[19] *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents,* GAO-22-104746 (Washington, D.C.: Jan. 13, 2022).

operations and assets of the agency. FISMA requires agencies to comply with OMB's policies and procedures, DHS's binding operational directives, and NIST's federal information standards and guidelines.[20]

FISMA also directs OMB to oversee agencies' information security policies and practices. Among other things, FISMA requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems.[21] The act further assigns OMB the responsibility of requiring agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agencies' information or information systems.

In addition, FISMA clarifies and expands DHS's responsibilities for government-wide information security. Specifically, the act requires DHS, in consultation with OMB, to oversee the implementation of agency information security policies and practices for non-national security information systems by: (1) assisting OMB in carrying out its oversight responsibilities; (2) developing, issuing, and overseeing the implementation of binding operational directives; and (3) providing operational and technical assistance. CISA, a component of DHS, issues binding operational directives and works in concert with the larger department to develop the CIO FISMA metrics.

Further, pursuant to FISMA, NIST is responsible for developing standards and guidelines that include minimum information security requirements. In working with OMB to develop these standards and guidelines, NIST is

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

[21] The Secretary of Defense and the Director of the National Security Agency jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks. The Executive Agent is responsible for coordinating with the Committee on National Security Systems to develop effective technical safeguarding policies and standards that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves. The heads of agencies that own or use national security systems are responsible for ensuring that the Committee's policies and directives are implemented within their agencies. See Executive Order 13587, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 7, 2011).

required to consult with federal agencies and other organizations to improve information security and privacy, avoid unnecessary and costly duplication of effort, and help ensure that its publications are complementary with the standards and guidelines used for the protection of national security systems.

FISMA also includes reporting requirements for IGs and federal agencies. Specifically, FISMA requires agency IGs to annually assess the effectiveness of the information security policies, procedures, and practices of their parent agency.[22] In addition, the act requires agencies to report annually to OMB, DHS, certain congressional committees, and the Comptroller General on the adequacy and effectiveness of their information security policies, procedures, and practices. The act further requires OMB, in consultation with DHS, to report to Congress annually 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.

## Federal Agencies and Inspectors General Are to Use NIST's Framework to Report on FISMA Implementation

NIST's Cybersecurity Framework is a tool for aligning policy, business, and technological approaches with managing cybersecurity risk.[23] In May 2017, Executive Order 13800 directed each executive branch agency to use the Cybersecurity Framework to manage its cybersecurity risks.[24] In addition, agencies and their IGs use the Cybersecurity Framework in reporting on the effectiveness of agency information security policies and practices and the implementation of FISMA and government-wide cybersecurity targets such as those related to the cybersecurity initiative within the IT Modernization CAP goal. The metrics used for FISMA reporting correspond to the core functions outlined in the Cybersecurity Framework.

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

[23] The Framework was developed in response to a 2013 executive order, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, (Washington, D.C.: Feb. 12, 2013). It was originally intended for use in protection of critical infrastructure. NIST initially issued guidance in February 2014 and has since revised the framework. See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (Gaithersburg, MD: Apr. 16, 2018).

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

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

The NIST Cybersecurity Framework is based on five core security functions.

- **Identify.** Develop an understanding of the organization's ability to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **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.[25]
- **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, the five functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

## CIOs Assess Agencies' Progress in Implementing Cybersecurity-Related CAP Goal Targets

As part of their FISMA reporting for fiscal years 2020 and 2021, agencies were to inform oversight bodies of their progress in meeting the targets related to the cybersecurity initiative within the IT Modernization CAP goal. The aim of the cybersecurity initiative is to mitigate the risk and impact of threats to federal agencies' data, systems, and networks by implementing cutting edge cybersecurity capabilities. The initiative consisted of three strategies:

- The manage asset security strategy requires agencies to implement capabilities that provide observational, analytical, and diagnostic data of an agency's cybersecurity.
- The limit personnel access strategy requires agencies to implement credential and access management capabilities to ensure that users only have access to the resources necessary for their job function.

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

- The protect networks and data strategy requires agencies to implement advanced capabilities to protect agency networks and sensitive government and citizen data.

Included among these strategies were a total of 10 targets with corresponding milestones, as shown in the table below.

**Table 1: The Cybersecurity-Related Cross-Agency Priority (CAP) Goal Targets and Their Due Dates, as of the End of Fiscal Year 2020**

| Strategy | Key Milestone | Target | Target Due Date |
|---|---|---|---|
| Manage asset security by implementing capabilities that provide observational, analytical, and diagnostic data of an agency's cybersecurity. | Software asset management | 95% of software assets are covered by a whitelisting capability.[a] | September 2020 |
| | Hardware asset management | 95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset. | September 2020 |
| | Authorization management | 100% of high and moderate impact systems are covered by a valid security authorization to operate. | September 2020 |
| | Mobile device management | 95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised. | September 2020 |
| Limit personnel access by implementing credential and access management capabilities that ensure users only have access to the resources necessary for their job function. | Privileged network access management | 100% of privileged users are required to use a personal identity verification (PIV)[b] card or authenticator assurance level three (AAL3)[c] multifactor authentication method to access the agency's network. | September 2018 |
| | High-value asset access management | 90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method. | September 2020 |
| | Automated access management | 95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels. | September 2020 |
| Protect networks and data by implementing advanced network and data protection capabilities to protect agency networks and sensitive government and citizen data. | Intrusion detection and prevention | At least four of six intrusion prevention metrics have met an implementation target of at least 90%, and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source. | September 2020 |
| | Exfiltration and enhanced defenses | At least three of four exfiltration and enhanced defenses metrics have met an implementation target of at least 90%. | September 2020 |
| | Data protection | At least four of six data protection metrics have met an implementation target of at least 90%. | September 2020 |

Source: GAO analysis of the fiscal year 2021 chief information officer *Federal Information Security Modernization Act of 2014* metrics and the President's Management Agenda as of September 2020. | GAO-22-104364

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

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

[c] Authenticator assurance level three uses a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.

OMB included the targets in the fiscal year 2021 CIO FISMA metrics, allowing agency CIOs, OMB, and DHS to monitor agencies' continued progress in meeting them. The CIO FISMA metrics were intended to allow agencies and oversight bodies to assess agencies' progress toward achieving outcomes and targets that strengthen federal cybersecurity, such as those related to the cybersecurity-related CAP goal targets. Since fiscal year 2016, OMB and DHS have organized the CIO FISMA metrics around the NIST Cybersecurity Framework. The FISMA metrics leverage the Cybersecurity Framework as a standard for managing and reducing cybersecurity risks, and they are organized around the framework's five functions.

## Inspectors General Are Required to Determine the Effectiveness of Agencies' Information Security Programs

IGs are to assess and report on the effectiveness of their agencies' information security programs by using a capability maturity model developed by OMB, DHS, and CIGIE, in collaboration with other stakeholders. According to the fiscal year 2020 and 2021 IG FISMA metrics guidance, one of the goals of the maturity model reporting approach is to ensure consistency in IG FISMA evaluations across the federal government. As shown in table 2, the maturity model identifies five maturity levels, with each succeeding level representing a more advanced level of implementation.

**Table 2: Inspector General Evaluation Maturity Levels for Assessing Agencies' Information Security Programs**

| Maturity Level | Description |
|---|---|
| Level 1: Ad Hoc | Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner. |
| Level 2: Defined | Policies, procedures, and strategies are formalized and documented, but not consistently implemented. |
| Level 3: Consistently Implemented | Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. |
| Level 4: Managed and Measurable | Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes. |

| Maturity Level | Description |
|---|---|
| Level 5: Optimized | Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs. |

Source: GAO analysis of *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021. | GAO-22-104364

Using the five-level maturity model described above, the IGs are to assign a maturity level rating for each of the five Cybersecurity Framework core security functions. In order to help them determine the ratings, IGs assess their agencies' implementation of activities and controls associated with each function using metrics developed by OMB and DHS in collaboration with CIGIE.[26] After determining the maturity levels of the core security functions, the IGs rate their agencies' overall information security programs as either effective or not effective.

Within the context of the maturity model, a Level 4 (Managed and Measurable) rating is the threshold for an effective level of security at the function and overall program level.[27] A core security function or information security program rated at Level 3 (Consistently Implemented) or lower would likewise be considered not effective.[28] However, in order to provide greater flexibility for the IGs, the fiscal year 2020 and 2021 IG FISMA metrics guidance gives IGs the discretion to determine that a core security function or program is effective at a maturity level lower than Level 4 (Managed and Measurable).

[26] The annual IG FISMA metrics and reporting instructions are developed as a collaborative effort among OMB, DHS, and CIGIE. The metrics provide reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs. See *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1* (May 2021).

[27] *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1* (May 2021).

[28] 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.

## Agency, IG, and GAO Reports Highlight Agencies' Uneven Effectiveness in Implementing Cybersecurity Requirements

In fiscal year 2020, the 23 civilian CFO Act agencies reported progress toward meeting the cybersecurity-related CAP goal targets; nevertheless, a majority of the agencies reported not fully meeting the targets.[29] In addition, IGs rated the majority of these 23 agencies as having ineffective IT security programs. Further, in our recent reports, issued from fiscal year 2019 through fiscal year 2021, we identified significant weaknesses in both government-wide cybersecurity initiatives and individual CFO Act agencies' IT security programs.

### Agencies Reported Progress, but Most Did Not Fully Meet Cross-Agency Priority Goal Targets

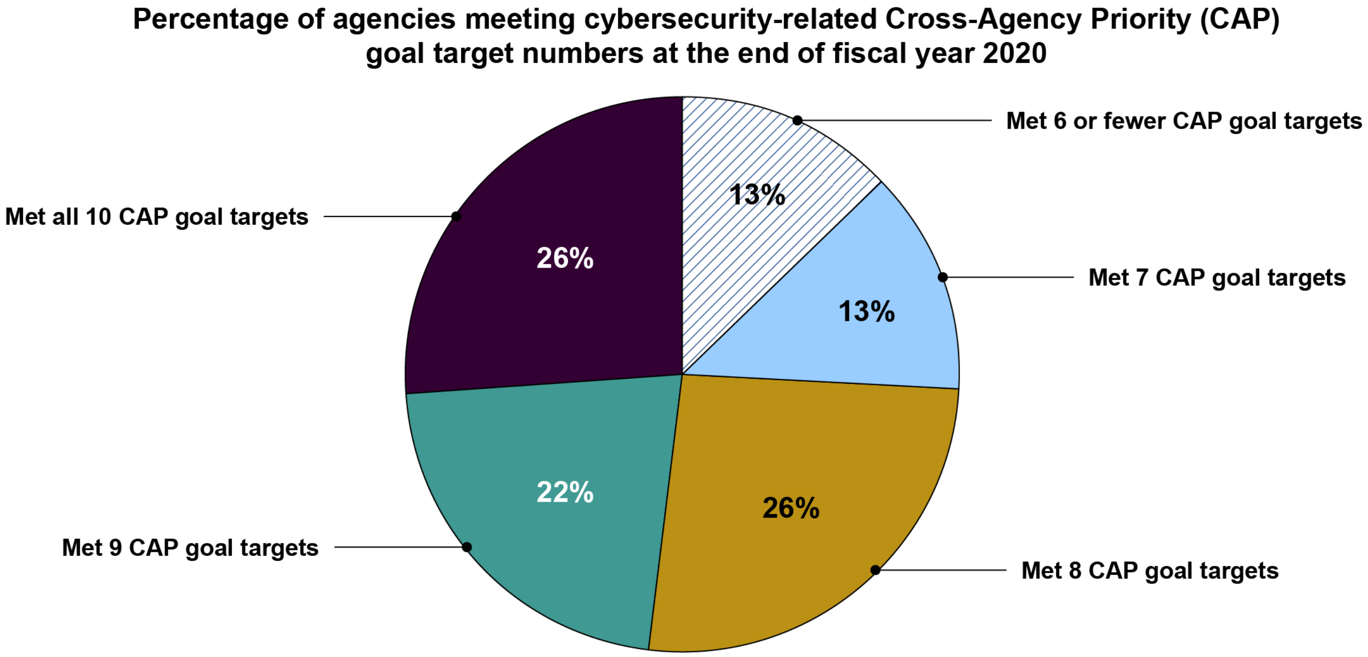
Between fiscal year 2018 and fiscal year 2020, the 23 civilian CFO Act agencies' FISMA reports indicated that, combined, the agencies made progress in meeting the cybersecurity-related targets for the IT Modernization CAP goal. While not all individual agencies reported progress over the 2-year period, the overall number of agencies that reported meeting all or most of the targets increased.

- The number of agencies reporting to have met between seven and 10 targets went up from 12 agencies (or 52 percent) in fiscal year 2018 to 20 agencies (or 87 percent) in fiscal year 2020.
- The number of agencies that reported meeting six or fewer targets decreased from 11 (or 48 percent) in fiscal year 2018 to three (or 13 percent) in fiscal year 2020.

Even with these increases, 17 of the 23 agencies did not meet all of the CAP goal targets in fiscal year 2020. Figure 3 depicts the agencies' reported status in meeting the cybersecurity-related CAP goal targets, as of the end of fiscal year 2020.

[29] The 23 civilian CFO Act agencies include all of the CFO Act agencies except for DOD. DOD is not included in this section of the report due to data sensitivity concerns.

**Figure 3: Percentage of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies Meeting the Cybersecurity-Related Cross-Agency Priority (CAP) Goal Targets, as of the End of Fiscal Year 2020**



Source: GAO analysis of agency fiscal year 2020 *Federal Information Security Modernization Act of 2014* reports. | GAO-22-104364

The collective performance data for fiscal year 2018 through fiscal year 2020 also shows that the agencies reported overall progress in meeting the IT Modernization CAP goal targets. The most significant gains over these years were in meeting the targets associated with the intrusion detection and prevention and software asset management milestones, which saw reported increases of 11 and eight agencies, respectively.

Despite this progress, none of the targets were fully met by all 23 agencies at the end of fiscal year 2020. The mobile device management milestone's target was the closest to being met by all 23 agencies, with 22 agencies reporting that they met the goal. The target associated with the high-value asset access management milestone was met by the fewest agencies, with 15 of the 23 agencies reporting that they met the goal in fiscal year 2020.

Table 3 shows the key milestones and targets related to the IT Modernization CAP goal's cybersecurity initiative, as well as how many agencies were meeting the targets at the ends of fiscal years 2018 through 2020.

**Table 3: Number of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies Meeting Cybersecurity-Related Cross-Agency Priority (CAP) Goal Targets at the Ends of Fiscal Years 2018, 2019, and 2020**

| | | Number of agencies that reported meeting targets by end of fiscal year | | |
|---|---|---|---|---|
| **Key Milestone** | **Target** | **2018** | **2019** | **2020** |
| Software asset management | 95% of software assets are covered by a whitelisting capability.[a] | 10 | 15 | 18 |
| Hardware asset management | 95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset. | 16 | 15 | 17 |
| Authorization management | 100% of high and moderate impact systems are covered by a valid security authorization to operate. | 14 | 17 | 16 |
| Mobile device management | 95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised. | 19 | 23 | 22 |
| Privileged network access management | 100% of privileged users are required to use a personal identity verification (PIV)[b] card or authenticator assurance level three (AAL3)[c] multifactor authentication method to access the agency's network. | 18 | 19 | 18 |
| High-value asset access management | 90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method. | 14 | 16 | 15 |
| Automated access management | 95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels. | 15 | 18 | 19 |
| Intrusion detection and prevention | At least four of six intrusion prevention metrics have met an implementation target of at least 90%, and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source. | 7 | 14 | 18 |
| Exfiltration and enhanced defenses | At least three of four exfiltration and enhanced defenses metrics have met an implementation target of at least 90%. | 23[d] | 20 | 20 |
| Data protection | At least four of six data protection metrics have met an implementation target of at least 90%. | 16 | 14 | 17 |

Source: GAO analysis of the fiscal year 2021 chief information officer *Federal Information Security Modernization Act of 2014* metrics, the President's Management Agenda as of September 2020, and Office of Management and Budget data on agencies' CAP goal performance. | GAO-22-104364

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

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

[c] Authenticator assurance level three uses a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.

[d] According to OMB, the vast majority of agencies (93 total agencies, including all 23 civilian CFO Act agencies) had met three of the four original targets set in the Exfiltration and enhanced defenses milestone in fiscal year 2018, and OMB considered the target to be achieved. OMB stated that, as a result, the target was shifted to the remaining metric concerning exfiltration detection (see CIO FISMA Metric 3.8).

As shown in table 3, the agencies' combined progress toward meeting the cybersecurity CAP goal targets generally improved between fiscal year 2018 and fiscal year 2020. Specifically, the fiscal year 2020 figures showed overall improvement in meeting eight of the ten targets when compared to the fiscal year 2018 numbers.

Of the two remaining targets, one target was met by the same number of agencies in fiscal year 2018 as in fiscal year 2020, and the other target was met by three fewer agencies in both fiscal years 2019 and 2020 than in fiscal year 2018. According to a statement made by OMB officials, the decreased number of agencies meeting the latter target is not evidence of regression. Specifically, as noted in table 3, the officials informed us that fewer agencies met the target in fiscal years 2019 and 2020 because OMB changed the original target after fiscal year 2018.

## Inspectors General Rated Seven of 23 Agencies as Having Effective IT Security Programs in Fiscal Year 2020

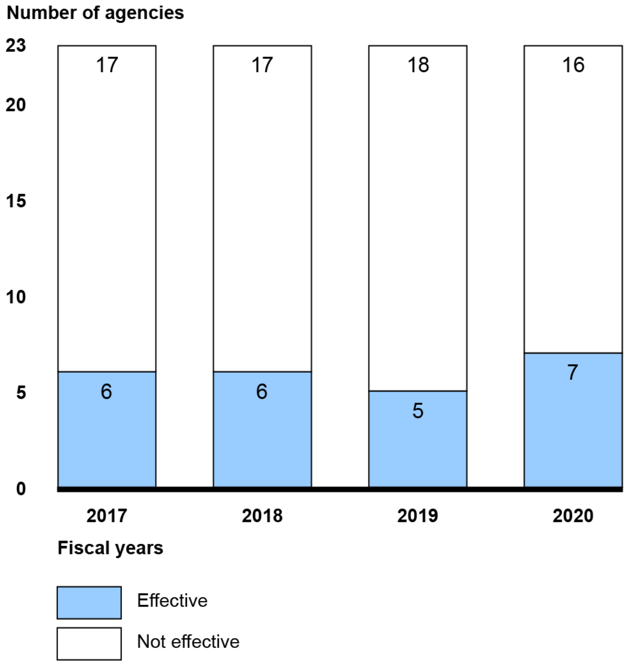
As mentioned earlier, IGs are to assess and report on the effectiveness of their agencies' information security programs using a capability maturity model developed by OMB, DHS, and CIGIE. The model identifies five maturity levels—from Level 1 (Ad Hoc) to Level 5 (Optimized)—with each succeeding level representing a more advanced level of program implementation.

In their fiscal year 2020 FISMA reports, IGs noted that seven (or 30 percent) of the 23 civilian CFO Act agencies had effective information security programs: DHS, Energy, the Environmental Protection Agency (EPA), the General Services Administration (GSA), the Nuclear Regulatory Commission (NRC), the National Science Foundation (NSF), and the U.S. Agency for International Development (USAID). Conversely, the IGs reported that 16 (or 70 percent) of the agencies had ineffective security programs in fiscal year 2020.

The total number of civilian CFO Act agencies receiving effective ratings has remained fairly consistent over the four most recent annual assessments: each year, 22 to 30 percent of the agencies received effective ratings. Specifically, for both fiscal years 2017 and 2018, the IGs rated six of the 23 agencies' programs as effective. In fiscal year 2019, the number of agencies receiving effective ratings decreased by one. In fiscal year 2020, the number of agencies with effective ratings increased by two, bringing the total to seven—only one agency more than in fiscal year 2017. In addition to the total number of agencies receiving effective ratings remaining relatively constant, the specific agencies receiving those effective ratings has also remained relatively constant.

Figure 4 shows the number of the 23 agencies that IGs rated as effective and not effective between fiscal years 2017 and 2020.

**Figure 4: Number of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies with Effective and Not Effective Agency-Wide Information Security Programs, as Reported by Inspector Generals for Fiscal Years 2017-2020**



Source: GAO analysis of inspector general report data and Office of Management and Budget's *Federal Information Security Modernization Act of 2014* reports to Congress. | GAO-22-104364

Table 4 shows the individual maturity ratings by core security function area for each of the 23 agencies, as well as the IGs' overall effectiveness ratings.

**Table 4: Inspector General (IG) Maturity Level and Overall Ratings of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies' Information Security Programs, as Reported in the IGs' *Federal Information Security Modernization Act of 2014* (FISMA) Fiscal Year 2020 Assessments**

| | Maturity level ratings for the five core security functions | | | | | |
|---|---|---|---|---|---|---|
| **Agency** | **Identify** | **Protect** | **Detect** | **Respond** | **Recover** | **Overall security program rating[a]** |
| Department of Agriculture | 3 | 3 | 2 | 4 | 2 | Not effective |
| Department of Commerce | 2 | 2 | 2 | 2 | 2 | Not effective |
| Department of Education | 2 | 2 | 2 | 3 | 3 | Not effective |
| Department of Energy | 3 | 3 | 3 | 4 | 3 | Effective |
| Department of Health and Human Services | 3 | 3 | 3 | 3 | 2 | Not effective |
| Department of Homeland Security | 4 | 3 | 4 | 3 | 1 | Effective |
| Department of Housing and Urban Development | 3 | 2 | 2 | 3 | 3 | Not effective |
| Department of Justice | 3 | 4 | 3 | 4 | 3 | Not effective |
| Department of Labor | 3 | 4 | 3 | 4 | 3 | Not effective |
| Department of State | 2 | 3 | 1 | 4 | 2 | Not effective |
| Department of the Interior | 3 | 4 | 3 | 4 | 3 | Not effective |
| Department of the Treasury | 3 | 3 | 3 | 4 | 3 | Not effective |
| Department of Transportation | 2 | 2 | 2 | 3 | 2 | Not effective |
| Department of Veterans Affairs | 2 | 2 | 2 | 4 | 2 | Not effective |
| Environmental Protection Agency | 3 | 3 | 3 | 3 | 3 | Effective |
| General Services Administration | 4 | 4 | 5 | 4 | 3 | Effective |
| National Aeronautics and Space Administration | 2 | 2 | 2 | 3 | 3 | Not effective |
| National Science Foundation | 5 | 4 | 4 | 4 | 5 | Effective |
| Nuclear Regulatory Commission | 4 | 4 | 4 | 4 | 3 | Effective |
| Office of Personnel Management | 1 | 3 | 2 | 4 | 2 | Not effective |
| Small Business Administration | 2 | 3 | 2 | 4 | 3 | Not effective |
| Social Security Administration | 2 | 2 | 2 | 4 | 2 | Not effective |
| U.S. Agency for International Development | 4 | 4 | 4 | 4 | 3 | Effective |

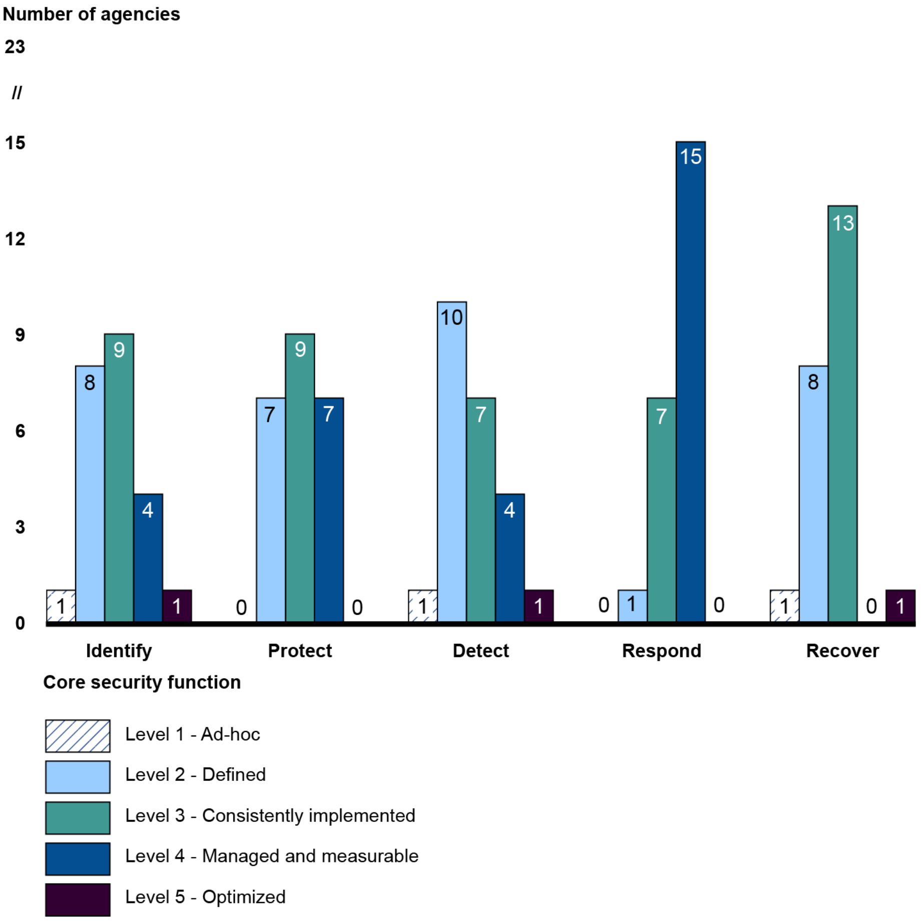
Key: The five maturity levels, from the least to the most mature, are: Level 1 (Ad Hoc); Level 2 (Defined); Level 3 (Consistently Implemented); Level 4 (Managed and Measurable); and Level 5 (Optimized).

Source: GAO analysis of inspector general report data and OMB's fiscal year 2020 FISMA report to Congress. | GAO-22-104364

[a] OMB strongly encouraged—but did not require—IGs to rate their agency's overall information security program as effective if three or more of the five core security functions are also rated as effective (i.e., above a Level 3 [Consistently Implemented]). Conversely, OMB encouraged IGs to rate their agency's security program as not effective if the ratings did not meet this threshold. IGs ultimately had the discretion to determine the overall effectiveness rating.

With regard to the five core security functions, in fiscal year 2020, the IGs rated most of the 23 agencies as not effective (i.e., lower than Level 4 [Managed and Measurable]) for four of the functions: Identify, Protect, Detect, and Recover. Specifically, the IGs rated 18 agencies as not having an effective Identify function, 16 agencies as not having an effective Protect function, 18 agencies as not having an effective Detect function, and 22 agencies as not having an effective Recover function. Conversely, for the remaining function, Respond, the majority of the agencies received effective ratings, with eight agencies being rated as not effective. Figure 5 shows the number of agencies receiving a particular maturity rating in each of the five core security functions.

**Figure 5: Fiscal Year 2020 Inspector General Ratings of the 23 Civilian *Chief Financial Officers Act of 1990* Agencies' Cybersecurity Framework Core Security Functions**



Source: GAO analysis of agency fiscal year 2020 *Federal Information Security Modernization Act of 2014* reports. | GAO-22-104364

Note: According to the Office of Management and Budget's fiscal year 2021 IG FISMA reporting metrics guidance, a rating of Level 4 (Managed and Measurable) or Level 5 (Optimized) is considered an effective level of security. A core security function rated at Level 3 (Consistently Implemented) or lower is considered not effective.

Regarding individual agencies' IG assessments, three agencies (DHS, NSF, and USAID) had at least one of their five core security functions' fiscal year 2020 ratings increase by two levels or more. One agency, DHS, had a security function rating that lowered by two levels or more.

- DHS's IG ratings for its Identify, Detect, and Respond security functions increased by at least two levels from fiscal year 2019 to fiscal year 2020. Specifically, DHS's Identify and Detect ratings increased from a Level 1 (Ad Hoc) to a Level 4 (Managed and Measurable), and the Respond rating increased from Level 1 (Ad Hoc) to a Level 3 (Consistently Implemented).

According to the DHS IG, the department's fiscal year 2019 ratings were affected by the DHS CIO's June 2019 decision to permit the Coast Guard to submit its cybersecurity and FISMA reports to DOD.[30] The IG stated that DHS's decision adversely affected the department's information security program in certain key areas, such as risk management and incident reporting. The IG also stated that, due to this change, the department's senior officials could not consistently capture qualitative and quantitative performance measures or monitor security controls effectively.

Conversely, in the IG's fiscal year 2020 independent assessment, the DHS IG stated that the Coast Guard was not part of DHS's fiscal year 2020 ratings. The exclusion of the Coast Guard meant that any associated issues with its reporting were not considered and, therefore, the department's ratings improved.

DHS's IG rating for the Recover function decreased by two levels to a Level 1 (Ad Hoc). According to the IG's public report, DHS received the lowest rating for this function because the department's Information System Contingency Planning Manager position was vacant in fiscal year 2020.[31]

- NSF's IG rating for the Identify and Recover functions increased by two levels to Level 5 (Optimized) in fiscal year 2020. When asked about these increases, NSF officials stated that their continuous monitoring program allows them to identify and evaluate risks and plan appropriate mitigation strategies. They also noted that NSF's recovery planning is integrated with NSF's overall IT risk management approach and that NSF has committed the resources for an effective continuity of operations capability.
- USAID's IG rating for the Protect security function increased by two levels to a Level 4 (Managed and Measurable) in fiscal year 2020. According to a USAID official within the Office of the CIO, the improved IG rating is a demonstration of the last several years of work that USAID has performed to align the agency's information security

[30] The Coast Guard is a component of DHS.

[31] DHS Office of Inspector General, *Evaluation of DHS' Information Security Program for Fiscal Year 2020*, OIG-21-72 (Washington, D.C.: Sept. 30 2021).

program with FISMA. The official added that a consistent methodology from year to year helps to prepare USAID for the audit and to know what to expect.

## Recent GAO Reports Highlight Actions Needed for Agencies to Improve Their Cybersecurity Programs

As part of our oversight of federal information security, we conducted numerous reviews from October 2018 through May 2021 to assess federal agencies' cybersecurity, including their implementation of FISMA requirements. These reviews have identified weaknesses in both government-wide cybersecurity initiatives and the information security programs at individual agencies. Consequently, we made recommendations to address these weaknesses.

### Recent GAO Reports Identified Weaknesses in Government-Wide Cybersecurity Programs and Initiatives

#### Agencies Improved Cybersecurity Risk Management, but Challenges to Implementing Key Practices Remain

FISMA requires agencies to assess the risk and magnitude of the harm resulting from unauthorized access or misuse of their information or information systems. The law also requires agencies to implement policies and procedures to cost-effectively reduce any risks to an acceptable level. Further, FISMA and federal policies emphasize that agencies take a risk-based approach to cybersecurity by identifying, prioritizing, and managing their cyber risks.[32] Key practices for establishing an agency-wide cybersecurity risk management program include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management program.

[32] The federal policies that address cybersecurity risk management include: Office of Management and Budget, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, OMB M-22-05 (Washington, D.C.: Dec. 6, 2021); Executive Order 14028, *Improving the Nation's Cybersecurity* (Washington, D.C, May 12, 2021); Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Washington, D.C.: May 11, 2017); Office of Management and Budget*, Managing Information as a Strategic Resource,* OMB Circular A-130 (Washington D.C.: July 28, 2016); and Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control,* OMB Circular A-123 (Washington, D.C.: July 15, 2016).

In July 2019, we reported that the 23 civilian CFO Act agencies varied in the extent to which they had established key elements of their cybersecurity risk management programs.[33] Specifically, 22 of 23 agencies had established the role of cybersecurity risk executive, and all 23 agencies had at least partially established policies that addressed key management elements such as assessing, responding to, and monitoring risk. However, 16 of 23 agencies had not fully established a cybersecurity risk management strategy, and six of 23 agencies had fully established risk management policies and procedures. As shown in table 5, the agencies identified challenges in establishing a cybersecurity risk management program, such as those related to hiring and retaining key personnel.

**Table 5: Challenges Identified by the 23 Civilian *Chief Financial Officers Act of 1990* Agencies in Developing and Implementing Cybersecurity Risk Management Programs**

| Challenge | Agencies reporting challenge |
|---|---|
| Hiring and retaining key cybersecurity risk management personnel | 23 |
| Managing competing priorities between operations and cybersecurity | 19 |
| Establishing and implementing consistent cybersecurity risk management policies and procedures | 18 |
| Establishing and implementing standardized technology capabilities | 18 |
| Receiving quality risk data | 18 |
| Using National Institute of Standards and Technology and Office of Management and Budget federal cybersecurity risk management guidance | 16 |
| Developing an agency-wide risk management strategy | 15 |
| Incorporating cyber risks into enterprise risk management | 14 |

Source: GAO analysis of agency data. | GAO-22-104364

Accordingly, we recommended that OMB establish guidance to facilitate information sharing regarding agencies’ successful approaches to address challenges in several risk management areas. We also made 57 recommendations to the 23 civilian CFO Act agencies to improve their

[33] GAO-19-384.

cybersecurity risk management policies and procedures. As of March 2022, OMB and the 23 civilian CFO Act agencies had not yet implemented 24 of the 58 recommendations.

### Agencies Increased the Authorization of Cloud Services, but Challenges Remained with Program Implementation

FISMA requires that agencies ensure the security of information and systems maintained by third parties on their behalf, including cloud systems. Cloud computing relies on internet-based interconnectivity and resources to provide computing services to customers, while intending to free customers from the burden and costs of maintaining the underlying infrastructure.

OMB established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to securing systems, assessing security controls, and continuously monitoring cloud services used by federal agencies. Before agencies issue subsequent authorizations for using cloud services that process, transmit, or store government information, agencies are responsible for ensuring that these cloud services use FedRAMP's baseline security controls.

In December 2019, we reported on the implementation of FedRAMP requirements at 24 federal agencies.[34] We noted that, while these agencies had increased the number of FedRAMP authorizations of cloud services by 137 percent from 2017 to 2019, 15 agencies had reported using cloud services that were not authorized by the program, as required by OMB.

In addition, we noted that four selected agencies did not consistently address key elements of the FedRAMP authorization process. Specifically, these key elements were addressing required information in security plans, summarizing control tests in security assessment reports, including required information in remedial action plans, and providing cloud service authorizations to the FedRAMP Program Office.

Further, agencies reported improved data security but also reported challenges such as not having sufficient resources to comply with the program. GSA had taken steps to improve FedRAMP, but its guidance on requirements and responsibilities was not always clear, and the

[34] GAO-20-126.

program's process for monitoring the status of security controls over cloud services was limited. In addition, while OMB required the use of FedRAMP for authorizing cloud services, it did not effectively monitor agencies' compliance with this requirement. Consequently, we stressed that OMB may have less assurance that cloud services used by agencies would meet federal security requirements.

As a result, we made 25 recommendations: one recommendation to OMB to enhance oversight, two recommendations to GSA to improve guidance and monitoring, and 22 recommendations to the selected four agencies to address shortcomings with the management of their cloud services. As of March 2022, OMB and the agencies had implemented five of the 25 recommendations.

### Agencies Implementing DHS Directives Improved Their Information Security Programs, but Challenges Remained with Execution

FISMA authorized DHS, in consultation with OMB, to develop and oversee the implementation of binding operational directives. These directives require agencies to safeguard federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.

In February 2020, we reported on DHS's process for developing and overseeing the implementation of the security directives; we also reported on the effectiveness of the directives, as well as select agencies' implementation of directive requirements.[35] Specifically, we reported that DHS had issued directives, but had not fully followed a process to ensure that potential benefits were realized. Notwithstanding, we noted that the directives had often been effective at strengthening agencies' information security programs. For instance, agencies made reported improvements in securing or replacing vulnerable network infrastructure devices in response to a 2016 directive.

While we reported that DHS had defined a directive process, we also stressed that it needed to follow the process more closely. In addition, federal agencies had not always fully implemented directives in a timely manner. Thus, we made four recommendations to address shortcomings in DHS's implementation of its directive process, such as consulting stakeholders early during development and validating agencies'

[35] GAO-20-133.

implementation of the directives. As of March 2022, DHS had implemented all four recommendations.

### Agencies Did Not Fully Benefit from DHS's Government-Wide Network Monitoring Program

DHS established its Continuous Diagnostics and Mitigation (CDM) program to support government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity. The objectives of the CDM program are to

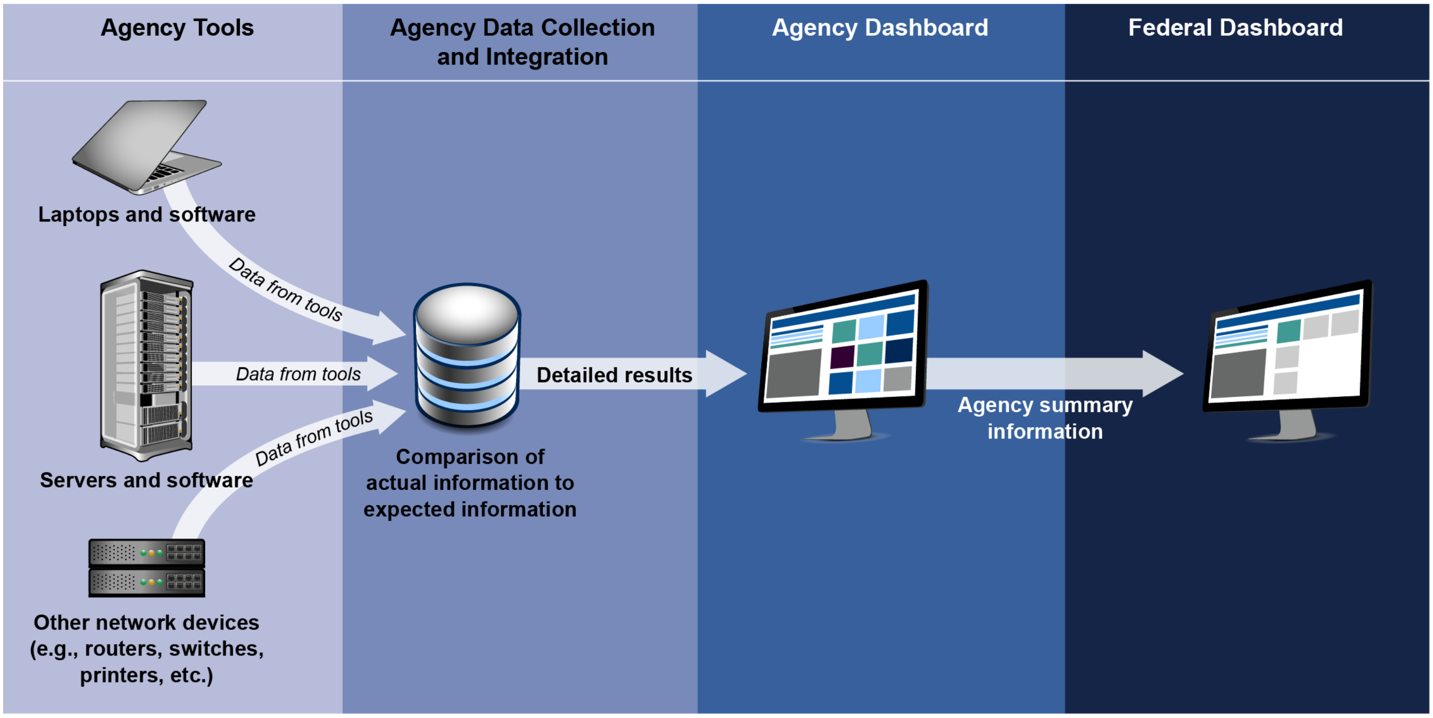
- reduce the agency threat surface;[36]
- increase visibility into the cybersecurity posture of agencies;
- improve an agency's ability to respond to cybersecurity issues; and
- streamline FISMA reporting.

The program is intended to allow federal agencies to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at both the individual agency and federal levels.

As depicted in Figure 6, the CDM program relies on automated tools to identify hardware and software residing on agency networks. The CDM tools aggregate this information and compare it to expected outcomes, such as whether actual device configuration settings meet federal benchmarks. The information is then displayed on an agency dashboard and federal dashboard. The agency dashboards display detailed information so agencies can use it to make decisions, and the federal dashboard presents summary information to help DHS effectively monitor security across the government.

[36] A threat surface consists of all hardware and software that may be exposed to compromise due to insecure configurations or known vulnerabilities. Keeping threat surfaces as small as possible is a basic security measure.

**Figure 6: Continuous Diagnostics and Mitigation Program Data Flow**


Agency Tools
Agency Data Collection and Integration
Agency Dashboard
Federal Dashboard
Laptops and software
Data from tools
Servers and software
Data from tools
Data from tools
Other network devices (e.g., routers, switches, printers, etc.)
Comparison of actual information to expected information
Detailed results
Agency summary information

Source: GAO analysis of Department of Homeland Security data. | GAO-22-104364

In August 2020, we reported that three agencies—the Federal Aviation Administration, the Indian Health Service, and the Small Business Administration—had generally deployed tools to support DHS's CDM program, but had not effectively implemented all key requirements.[37] Additionally, these agencies and three others—Justice, the Federal Deposit Insurance Corporation, and the Federal Communications Commission—had identified challenges to implementing CDM, such as a lack of resources and not having direct oversight of contractors. We reported that DHS had taken steps to address the agency-identified challenges, such as tracking risks and soliciting feedback on contractor performance.

We made 15 recommendations to improve DHS's management of the program and three agencies' implementation of the program. These recommendations addressed weaknesses that limited DHS's ability to

[37] GAO-20-598.

monitor agency information security. As of March 2022, DHS and the three agencies had implemented two of the 15 recommendations.

## Recent GAO Reports Identified Weaknesses in Agencies' Management of Their Information Security Programs

In addition to identifying weaknesses with government-wide cybersecurity efforts, we have also identified weaknesses in the implementation of individual agencies' cybersecurity requirements. In recent reports, we identified deficiencies in these areas and made recommendations to improve how agencies such as the Centers for Disease Control and Prevention (CDC), DOD, the Department of Housing and Urban Development (HUD), and IRS manage information security and the security of information shared with third-party providers.

### CDC Addressed Information Security Program Deficiencies

As we previously discussed, FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. For its part, CDC relies on effective information security controls to protect its systems and fulfill its mission of protecting the U.S. from health, safety, and security threats.

In December 2018, we reported on the extent to which the agency had taken corrective actions to address security program and technical control deficiencies that we had identified in a prior report issued in June 2018.[38] In that report, we made 195 recommendations to strengthen CDC's technical security controls and bolster its agency-wide information security program. Specifically, we recommended that the agency take 184 actions to resolve technical control deficiencies by implementing stronger access controls, encrypting sensitive data, configuring devices securely, applying patches in a timely manner, strengthening firewall rules, and implementing logging and monitoring controls more effectively, among other actions. We also made 11 recommendations for CDC to improve its information security program by, among other things, assessing risks as needed, documenting more detailed technical requirements, monitoring and assessing controls more comprehensively, and remediating deficiencies in a timely manner.

[38] GAO-19-70. This report is a public version of a GAO limited official use only report issued in June 2018. For the public report, GAO not only presented a public version of the June 2018 report, but also determined the extent to which CDC had taken corrective actions to address the report's recommendations.

CDC had implemented all of our recommendations by January 2021. By doing so, the agency helped to better protect its systems and sensitive information from unauthorized use, disclosure, modification, or disruption.

### DOD Had Not Fully Implemented Plans to Improve Cyber Hygiene

FISMA addresses increasing, evolving, and ever more sophisticated cybersecurity threats by requiring agencies to provide security for their information systems in a manner commensurate with risk. Further, as previously discussed, FISMA requires agencies to submit annual reports that assess the adequacy of their information security policies, procedures, and practices.

In April 2020, we reported on DOD's efforts to implement initiatives and practices to manage the most common cybersecurity risks and improve cyber hygiene.[39] Carnegie Mellon University's Software Engineering Institute defines cyber hygiene as a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.[40]

According to a prior testimony from DOD's Principal Cyber Advisor, cybersecurity experts estimate that about 90 percent of cyberattacks could be defeated by implementing basic cyber hygiene and sharing best practices.[41] However, DOD officials have stated that there is no commonly used definition for cyber hygiene in DOD doctrine.

In our April 2020 report, we noted that the department's plans to improve cyber hygiene included efforts to implement recommended initiatives aimed at remediating vulnerabilities, improving awareness of cyber threats, and reinforcing best practices; however, many efforts were incomplete and some had no entity responsible for implementation. As part of the cyber hygiene initiative, the department also had created a

[39] GAO-20-241.

[40] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* (2017).

[41] *A Review and Assessment of the Department of Defense Budget, Strategy, Policy, and Programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019: Hearing Before Subcommittee on Emerging Threats and Capabilities (House Armed Services Comm.)* 115th Cong. 4 (Apr. 11, 2018) (statement of Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor).

Cyber Hygiene Scorecard to measure compliance with DOD cybersecurity policies, procedures, standards, and guidelines.

We identified shortcomings in the department's management of the implementation of these initiatives and practices, such as not tracking all users who completed required security training and not providing complete status updates to senior leaders. Further, we noted that, while the department had used the Scorecard with the intention to meet the FISMA annual reporting requirement, the Scorecard did not provide information for 53 of the 69 CIO FISMA metrics included in the fiscal year 2019 CIO metrics guidance.

We made seven recommendations to DOD to improve the implementation of its cyber hygiene initiatives, to monitor the status of user security training more effectively, and to assess the extent to which senior leadership had adequate information to make risk-based decisions. As of March 2022, DOD had not fully implemented any of the seven recommendations.

### DOD Did Not Implement Comprehensive Plans for the Improvement of Its Financial Management Systems

FISMA and other federal laws and guidance call for agencies to implement security controls over their financial management systems.[42] In September 2020, we reported that, according to the DOD IG and independent auditors, data supporting the department's fiscal year 2019 financial statements were not reliable.[43] In addition, we pointed out that DOD had neither developed measures to track progress in remediating financial management system weaknesses nor reliably identified the systems that supported its financial statements. We also reported that the department had created a strategy that fully addressed three requirements for a comprehensive IT strategic plan, but did not fully include measures for tracking progress toward the strategy's goals.

[42] According to GAO's *Federal Information System Controls Audit Manual (FISCAM)*, the laws and guidance generally relevant to information security control audits of federal agencies include: FISMA, the *Federal Financial Management Improvement Act of 1996*, 31 U.S.C. 3512 note; the *Federal Managers' Financial Integrity Act of 1982*, 31 U.S.C. 3512 (c), (d); and FISMA implementation guidance. See GAO, *Federal Information System Controls Audit Manual (FISCAM),* GAO-09-232G (Washington, D.C.: Feb. 2, 2009).

[43] GAO-20-252.

Further, while DOD had developed a plan to address known IT deficiencies, the plan did not include performance goals. Moreover, we reported that DOD did not know how much it spent on the systems that supported its financial statements because it did not have a way to reliably identify these systems in its systems inventory and budget data.

We made six recommendations to DOD. Four of the recommendations were related to developing plans, targets, and measures to help ensure that the department's systems would support financial management activities. We also recommended that the department identify a complete list of its financial management systems. Further, we recommended that the department ensure that DOD limits investments in financial management systems to only what is essential to maintain functioning systems and help ensure system security until it implements the other five recommendations. As of March 2022, DOD had not implemented any of the six recommendations.

### HUD Did Not Provide Effective Oversight of Data Exchanged with Third-Party Entities

FISMA specifies requirements for agencies such as the Department of Housing and Urban Development (HUD) to protect systems and data, including systems operated by a contractor or other organization that collects or maintains information on behalf of the agency. To administer housing, community investment, and mortgage loan programs, HUD collects a vast amount of sensitive personal information and shares it with external entities, including federal agencies; contractors; and state, local, and tribal organizations.

In September 2020, we reported that HUD was not effectively protecting sensitive information exchanged with external entities, as required by FISMA.[44] We assessed HUD against four leading practices for overseeing such information: (1) requiring risk-based security and privacy controls, (2) independently assessing control implementation, (3) developing and implementing whatever corrective actions are needed, and (4) monitoring the implementation of controls. We determined that HUD had not independently assessed its implementation of security controls and had only minimally addressed the other three practices, as shown in table 6.

[44] GAO-20-431.

Table 6: Extent to which the Department of Housing and Urban Development's Policies and Procedures Addressed Leading Practices for Overseeing the Protection of Sensitive Information

| Leading Practice | Rating |
|---|---|
| Require Risk-based security and privacy controls | ◔ |
| Independently assess implementation of controls | ○ |
| Identify and track corrective actions needed | ◔ |
| Monitor progress implementation controls | ◔ |

Legend: ◔=Minimally addressed—leading practice was addressed to a limited extent; ○=Not addressed—leading practice was not addressed.

Source: GAO analysis of HUD data. | GAO-22-104364

Additionally, HUD was not fully able to identify all external entities that processed, stored, or shared sensitive information with its systems. Our work identified additional external entities beyond what HUD reported for 23 of 32 systems. HUD also did not track what types of sensitive information was shared with external entities.

As a result, we made five recommendations to HUD to ensure that its policies require risk-based security and privacy controls for external entities; ensure that its policies require independent assessments of external entities; and track the third parties that have access to HUD information. As of March 2022, HUD had not implemented any of the five recommendations.

### IRS's Information System Security Deficiencies Increased Risk to Financial Reporting and Taxpayer Data

FISMA requires agencies to protect information, including personal and financial data, in a manner commensurate with the risk and magnitude of the harm resulting from its unauthorized access, use, disclosure, modification, or disruption. Security deficiencies in the IRS's information systems are significant because they potentially increase the risk to the personal and financial data of U.S. taxpayers.

In May 2021, we reported on the information system security controls of IRS processing and management systems.[45] In the report, we highlighted newly identified and continuing deficiencies related to access controls and

[45] GAO-21-401R.

configuration management. For example, we noted that IRS did not always remove certain accounts and users in accordance with agency policy.

We made one recommendation in the publicly releasable report to improve IRS's security management. As of March 2022, IRS had not implemented the recommendation.

## Agency Officials Reported That FISMA Improved Their Cybersecurity Programs but Also Identified Impediments and Suggested Improvements

According to officials such as CIOs and chief information security officers (CISO) at each of the 23 civilian CFO Act agencies and DOD (henceforth referred to as the 24 CFO Act agencies), FISMA and its reporting process have enabled their agencies to improve the effectiveness of their information security programs. Even so, officials from most of the agencies identified impediments to implementing FISMA requirements and meeting the reporting metrics. In light of both these benefits and impediments, the officials made suggestions for improving the implementation of FISMA and its reporting process. These suggestions included increasing the focus on cybersecurity risk management, increasing automation, and reducing the frequency of reviews. The officials' suggestions about the FISMA assessment process indicated that IG ratings are inconsistent, a position supported by the lack of clear instructions in the OMB guidance regarding the process for determining agencies' ratings. Specifically, the flexibility built into the rating process guidance allows IGs to provide final ratings that are not based on consistent reasoning or support. This inconsistency complicates oversight bodies' ability to compare agencies' performance across the government. Further, the effective/not effective final rating scale itself does not adequately communicate the effectiveness of agencies' information security programs.

### Agency Officials Reported That FISMA Enabled Agencies to Improve Their Cybersecurity Programs

Officials such as CIOs and CISOs at all 24 CFO Act agencies stated that FISMA and the FISMA reporting process had helped their agencies improve their security posture. Specifically, officials at 14 agencies stated that FISMA had enabled their agencies to improve their information security programs' effectiveness to a great extent, and officials at 10 agencies said that FISMA had enabled their agencies to improve their security programs' effectiveness to a moderate extent.[46]

In responding to our interview questions, officials from all 24 agencies stated that FISMA had enabled them to improve the effectiveness of their information security programs. The officials identified a number of benefits to their security programs that were derived from FISMA. Many of the benefits identified were specific to agencies' unique experiences with implementing the law and its related reporting processes. The seven most common benefits identified by agency officials' are listed below.

- **Standardized security program requirements.** Agency officials at 10 of the 24 CFO Act agencies stated that FISMA was effective because it standardized their security program requirements. For instance, GSA officials said the key benefit of FISMA was formalizing what comprised an effective government cybersecurity program. The officials explained that, before FISMA, many competing groups defined cybersecurity practices. FISMA, they stated, established specific experts to issue guidance and a common baseline for the agencies.
- **Mandated security requirements.** Officials from four agencies responded that FISMA's status as a legal requirement provided the authority to take actions that helped improve their cybersecurity posture. For example, according to an IT official at the Department of Labor, FISMA's legal status gave the agency the authority needed to prioritize the implementation of information security requirements.
- **Helped justify cybersecurity requests to management.** Officials at four agencies stated that FISMA had helped them make convincing cybersecurity requests to management. For example, an IT official at the Social Security Administration (SSA) stated that FISMA requirements had enabled the Office of the CIO to more easily persuade agency management to agree to increased cybersecurity efforts across the agency.
- **Allowed for more effective communication within the agency.** Officials from four agencies discussed how FISMA had helped

[46] We asked the agency officials a multiple choice question about the extent to which FISMA enabled their respective agency to improve the effectiveness of its information security program. The possible answers were: (a) to a great extent, (b) to a moderate extent, (c) to a minimal extent or not at all, or (d) effectiveness decreased rather than improved. As described in the text above, all of the agencies' officials responded either (a) to a great extent or (b) to a moderate extent. None of the agency officials answered (c) to a minimal extent or not at all or (d) effectiveness decreased rather than improved.

improve communication about cybersecurity issues within their agencies. According to officials at HUD, the FISMA reporting process improved communication and coordination between the department's program offices. The officials credited the increased number of information security discussions necessitated by the reporting process as one of the reasons behind this improvement.

- **Allowed agency to track performance of the security program.** Officials at four agencies noted that FISMA allows them to track the performance of their security programs over time. For instance, an IT official at the Department of Commerce stated that FISMA has allowed for the viewing of cybersecurity information through various dashboards to get a sense of where the department stands. This, in turn, allows the department to identify and fill gaps to reduce risks.
- **Guided agency priorities and security efforts.** Four agencies' officials cited FISMA's ability to guide agency priorities and security efforts. For example, an IT official at NASA stated that FISMA requirements guide the agency's priorities and become technical requirements. The official stated that NASA uses the FISMA requirements to guide work on key foundational capabilities and enterprise services.
- **Established responsibilities and authorities related to the cybersecurity program.** Officials from four agencies stated that FISMA helped to establish cybersecurity responsibilities and authorities. For instance, an IT official at the Department of the Interior remarked that FISMA provides agency heads—and, by delegation, agency CIOs—the authorities to balance business needs and risks. The official stated that FISMA empowers the OMB Director and DHS Secretary to establish government-wide priorities and reporting criteria.

## Agency Officials Identified Impediments to Implementing FISMA Requirements

Although officials specified how FISMA had helped improve their agencies' cybersecurity posture, CIOs and CISOs at the 24 CFO Act agencies identified a number of impediments to their agencies' implementation of FISMA.[47] The agency officials' top three impediments are listed below.

- **Lack of resources.** Officials at 10 agencies stated that a lack of resources has hindered their ability to implement FISMA

[47] While we specifically asked about "impediments" to the agencies' implementation of FISMA requirements, the officials at one agency took issue with the term and listed "challenges" to FISMA implementation instead.

requirements. For instance, an IT official at the Department of Health and Human Services (HHS) stated that some of its operating divisions are consistently under-funded, which impedes the consistent implementation of IT security changes across the agency. The official noted that this lack of resources causes difficulties when the department tries to implement a new security policy across all of its operating divisions.

Further, an IT official at USAID stated that the primary impediment to that agency's implementation of FISMA is the limited resources available for information security. The official stated that FISMA-related work is time-intensive, limiting the resources available for operational cybersecurity activities, such as managing the firewall or responding to incidents.

- **FISMA audit focuses on compliance, not effectiveness.** Officials at six agencies expressed concerns that the FISMA reviews are too focused on compliance and are not focused enough on effectiveness. According to an IT official at SSA, an approach based on compliance becomes less helpful as a security program becomes more mature. The official stated that some requirements, such as security training, should be managed by evaluating risk, not compliance. For instance, the official noted that, even if one staff member has not completed security training, SSA would not be rated as compliant with that requirement. According to the official, the non-compliance rating means that SSA must prioritize expending resources to improve the FISMA rating rather than address other, potentially higher-risk, cybersecurity concerns.
- **Insufficient time for implementation of new requirements and remediation of findings.** Officials at four agencies stated that they did not have enough time to implement new requirements and/or remediate findings identified in the annual FISMA reviews before the next FISMA review starts. An IT official at the Department of Veterans Affairs (VA) said that it takes time to implement technical, cultural, and policy changes due to the department's geographic diversity, mission complexity, and size. The official specifically discussed the time frames assigned to implementing DHS's binding operational directives as not being sufficient, as the department is challenged to allocate resources and strategize quickly.

  In addition, an IT official at Education stated that the biggest impediment to FISMA implementation is the timing of the FISMA audits. The official stated that Education receives the audit findings from the previous year's report in October or November; it then develops a corrective action plan in December, only to have the next audit begin the following February. The official added that this does not leave much time to address recommendations, resulting in repeat findings.

## Agency Officials Suggested Ways to Improve the FISMA Reporting Process; DHS and IGs Generally Agreed with Most Suggestions

While officials at each of the 24 CFO Act agencies stated that FISMA had helped to improve their agencies' information security programs, they also provided a number of suggestions for improving the effectiveness of the FISMA metrics, annual evaluations, and reporting process. IG officials, including those representing CIGIE's Technology Committee and those from the greater IG community who provided feedback through the CIGIE Technology Committee, and DHS officials within CISA, agreed with the reasoning behind some of these suggestions, but not all.

Agency officials' five most commonly suggested changes for improving the effectiveness of FISMA reporting are discussed below, along with related views from IG officials and DHS officials within CISA.

- **Update the metrics to increase their effectiveness.** Officials at 11 of the 24 CFO Act agencies offered various suggestions for updating the FISMA metrics and keeping them current to enhance their effectiveness. In addition to general suggestions to update out-of-date metrics, agency officials discussed changing how metrics were scored, as well as adding metrics related to specific cybersecurity concerns. For instance, an IT official at VA suggested an additional evaluation of the effectiveness and the impact of the existing metrics, as some of them are nearly a decade old.

  Other agency officials suggested that the metrics should be updated to account for unique factors such as mission-based technical capabilities and agency size. For example, an IT official at NASA suggested that the metrics include additional response categories to allow for differences in the agencies' technical capabilities. The NASA official explained that, since their systems run on a different operating system than most government systems, the agency may not always have a way to be 100 percent in compliance with the metrics.

  An IT official at Education had a similar suggestion to allow the IG metrics to be adapted to agency-specific circumstances. Specifically, the Education official stated that there should be discussions related to organizational size and complexity because these factors may determine the threshold for effectiveness.

  The IG officials who responded to the agency officials' suggestions through CIGIE's Technology Committee generally agreed with the idea to change or update the metrics to keep them useful, up-to-date, and effective. While IG officials work with OMB and DHS to assess and incorporate new risks—like supply chain risk—into the metrics, guidance, and directives, some of the IG respondents agreed that the metrics could be streamlined to focus more on objectives, outcomes, and priority risk areas. However, other IG respondents remarked that there are benefits to keeping the metrics stable from year to year, such as allowing for comparisons of agency progress over time. Further, most IG respondents noted that OMB and DHS already work with CIGIE to update the metrics on an annual basis.

DHS officials within CISA who help develop the CIO metrics agreed with the suggestion to update the metrics, remarking that they work to update the CIO metrics annually. Specifically, the CISA officials stated that they update the CIO metrics to address threats and vulnerabilities and to remove out-of-date metrics. The officials stated that, during the annual update process, they obtain feedback about agencies' concerns via meetings and emails. The officials further noted that, while CISA considers all suggestions for improving the FISMA reporting process, it consults with OMB for the final disposition of any recommendations.

- **Focus FISMA reviews more on factors such as risk than compliance.** Officials at 10 agencies stated that the annual FISMA inspectors general audits should be focused less on compliance with the metrics and more on other factors such as risk management. According to an IT official in DHS's Office of the CIO, FISMA compliance is not always a true measure of risk. Explaining this point, the official stated that an agency may be compliant with all requirements, but still not be properly managing its security risks.

  Further, an IT official at NSF suggested shifting the emphasis of FISMA metrics from a quantitative compliance review to one focusing on management issues. The official noted that smaller agencies, such as NSF, are subject to the same FISMA metrics as larger departments, such as DHS. According to the official, a shift to focusing on management of information security programs would make the results of the FISMA reviews more comparable across the government, despite the differences in agency size.

  However, officials from two of the IG offices that responded to the suggestions through the CIGIE Technology Committee noted that moving away from compliance would make it more difficult to compare data across the government. Further, the majority of IG officials stated that the current framework provides a balance between compliance and risk management. Some IG officials explained that their agencies' information security programs (particularly with respect to the risk management program) might not be mature enough to transition away from the compliance-based reviews that are appropriate for lower maturity levels.

DHS officials within CISA stated that they agreed with the suggestion to focus on factors other than compliance. In March 2021, the officials informed us that they were considering ways to focus the fiscal year 2022 CIO metrics more on risk management factors than compliance. The officials also noted that new methodologies, such as risk quantification and alignment to current threats and cybersecurity challenges, are being explored. They explained that this would allow agencies to focus on meaningful work to reduce risk. Further, the officials stated that the usefulness of some of the current metrics had diminished due to evolving technologies, updated guidance, or lapsing government requirements.

In December 2021, OMB issued M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, which states that OMB is shifting the emphasis of FISMA reporting away from compliance in favor of risk management.[48] For instance, M-22-05 encourages IGs to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls.

- **Increase the use of automation.** Officials at eight agencies suggested that the FISMA reporting process include more automation. For instance, an IT official at Treasury stated that the FISMA process requires numerous data calls and that they have to gather and validate data from all of Treasury's bureaus on a monthly basis. The official noted that increasing automation would enable Treasury to reduce the burden associated with maintaining spreadsheets and manual data entry. Further, an IT official at State remarked that automating the process would enable the agency to track progress throughout the year.

  The IG officials who responded to the suggestions through the CIGIE Technology Committee generally agreed with this suggestion, noting that increased automation could improve the FISMA reporting process. Some IG officials noted that automation could reduce

[48] Office of Management and Budget, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, OMB M-22-05 (Washington, D.C.: Dec. 6, 2021).

compliance costs and potentially streamline the number of metrics. However, the IG officials did have concerns with the transition to automation. For instance, they stated that, since automation is associated with higher FISMA maturity levels, moving to an automated process might not be feasible until agencies have mature security programs.

The DHS officials at CISA agreed with the suggestion to increase automation and specifically advocated for increasing the automation of FISMA requirements in areas such as asset management. They explained that lessening agencies' dependency on manual processes would decrease the burden on the agencies to meet their reporting requirements and provide consistency in interpreting the results. The CISA officials also remarked that DHS's CDM program should automate many FISMA requirements as it matures. In March 2021, the CISA officials informed us that there had been discussions about increasing automation for the fiscal year 2022 CIO metrics. In July 2021, the CISA officials stated that an upcoming CDM release would enable the automated visualization of data related to select FISMA questions.[49]

The fiscal year 2021 IG FISMA metrics guidance proposed a change that may also result in an increased focus on automation. Specifically, the guidance introduced a pilot concept of weighting specific priority FISMA metrics twice as much in the maturity calculation. One of the proposed priority metrics is Metric 10: Automated view of risk.[50] The guidance explained that Metric 10 was chosen because meeting the metric would (1) improve the government's ability to report and

[49] As discussed above, CISA officials stated that the CDM program should automate many FISMA requirements as it matures. In the previously discussed August 2020 CDM report (GAO-20-598), we reported on foundational issues with the implementation of CDM at select agencies. For instance, we found that CDM tools at select agencies were not able to provide an accurate count of the hardware on the network. As we noted in the report, incorrect information about the number of devices undermines CDM's goal of streamlining FISMA reporting because several FISMA metrics depend on accurate device counts. Implementing the recommendations from the CDM report should help improve the CDM program and help the program achieve its stated goal of streamlining FISMA reporting.

[50] Metric 10 is "To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?" According to the guidance, an agency with a Level 5 (Optimized) score for this metric would have institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program. See *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1* (May 12, 2021).

analyze cybersecurity data for use in decision making and (2) support the administration's focus on automated reporting.

In addition, OMB's December 2021 guidance on information security and privacy management requirements states that OMB is emphasizing automation and the use of machine-readable data to speed up reporting, reduce agency burden, and improve outcomes. The guidance further directs the development of a strategy to enable agencies to report performance and incident data in an automated and machine-readable manner.

- **Improve the IG evaluation process and the maturity rating model.** IT officials from eight agencies suggested making changes to the IG evaluation process and the maturity ratings. For example, an IT official at Labor stated that the standard for an effective security program should be changed from Level 4 (Managed and Measurable) to Level 3 (Consistently Implemented). Likewise, an IT official at NSF stated that a program rated as "Consistently Implemented" sounds like it would be the result of a positive evaluation, not one resulting in an ineffective rating.

  Other agency officials suggested that the overall IG rating be changed to include additional graduated levels between effective and not effective to reflect the degree of effectiveness. For example, an IT official at HHS suggested that a gradient scale between effective and not effective might be useful because an IG rating of not effective might encourage attacks.

  In addition to changing the ratings themselves, other agency officials discussed inconsistencies in the IG evaluation process and in the manner in which IGs calculated the ratings. For instance, an IT official at GSA stated that uneven IG performance led to inconsistency across the FISMA assessments. The official noted that inconsistency could cause agencies with less effective security practices to receive higher scores on their FISMA audits than other agencies with more resilient real-world security programs. The official stated that the audits should be more standardized, and suggested the development of additional IG audit guidance.

  The majority of the IG officials who responded through the CIGIE Technology Committee agreed with the idea of being able to rate agencies with graduated levels of effectiveness. However, the majority of the IG officials did not agree with the suggestion that Level 3 (Consistently Implemented) be considered the threshold for effectiveness. The IG officials who favored the status quo noted that moving the compliance bar to Level 3 (Consistently Implemented) could result in agencies losing the incentive to implement the automation, monitoring, and feedback processes of the higher levels. IG officials did suggest that a Level 3 (Consistently Implemented) could possibly be “minimally effective” if agencies were rated on a graduated scale.

With regard to FISMA assessment inconsistency, an IG official representing the CIGIE Technology Committee stated that the Supplemental Guide to IG Metrics is a supplemental guide to help IGs with their assessments. He stated that the guide focuses on tests and artifacts for a Level 4 (Managed and Measurable) rating. While the guide has not been updated since fiscal year 2019, the fiscal year 2021 IG FISMA metrics guidance states that OMB, DHS, and CIGIE plan to update it.

Further, CISA officials supported this suggestion. In particular, the officials were in favor of developing a gradient rating scale.

- **Reduce the frequency of FISMA-required independent annual reviews/evaluations.** Officials at seven agencies recommended lessening the frequency of FISMA-mandated audits to reduce the burden of the annual review cycle. An IT official at USAID, for instance, stated that the agency only had between four and five months to address weaknesses identified by the annual FISMA audits before the next year’s audit started. Due to these tight timelines, the official suggested changing the frequency of FISMA reports to every other year in order to give the agency more time to work on remediation activities and long-term projects.

  Further, as previously mentioned, an IT official at Education stated that the biggest impediment to FISMA implementation was the timing of the FISMA audits. Specifically, the official noted that the FISMA report cycle does not leave much time to address any audit recommendations, resulting in repeat findings.

  However, the IG officials were split on whether reducing the frequency of the audits would improve FISMA or the reporting process. The IG respondents who supported this suggestion explained that fewer reviews could give agencies more time to address IG findings and reduce the burden of more mature agencies’ FISMA assessments. On the other hand, IG officials representing the CIGIE’s Technology Committee stated that they did not think that less frequent reviews would result in better cybersecurity. Other IG officials warned that reducing oversight might lead to additional breaches and cost. Instead, they suggested that a hybrid approach where frequency is tied to agency maturity might be a better solution.

Officials at CISA did not have an opinion on this proposed change. That said, they noted that increasing the amount of automation, as previously suggested, could mitigate the impact of the short time frames by reducing the amount of time required for manual data collection.

OMB's December 2021 guidance on information security and privacy management requirements may help to respond to this suggestion and the agencies' related concerns. According to the guidance, OMB will be implementing a new reporting cycle for the IG FISMA metrics. Specifically, it states that OMB will select a core group of prioritized metrics that will still be evaluated annually; the other metrics will be evaluated on a two year cycle on a calendar agreed to by OMB and its partners.

## Guidance for Rating the Effectiveness of Agencies' Programs Was Not Clear

FISMA requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies.[51] Each year, OMB, in partnership with DHS and CIGIE, develops metrics guidance for IGs' annual FISMA reports, which rate the effectiveness of their agencies' information security programs. The IG ratings help to inform the Congress and other oversight bodies on agencies' implementation of security.

As with its fiscal year 2020 guidance, OMB's 2021 IG FISMA report guidance instructed IGs to rate the effectiveness of their agencies' information security programs by assessing agencies' performance across each of the five core security functions within the Cybersecurity Framework. The fiscal year 2021 FISMA metrics guidance strongly encouraged IGs to rate their agency's information security program as effective or not effective by applying a rule of simple majority. Specifically, if three or more of the five core security functions were rated effective (i.e., rated at a Level 4 [Managed and Measurable] or Level 5 [Optimized]), the overall information security program would be rated as effective.

Despite OMB's strongly encouraged methodology, the metrics guidance also gave IGs the discretion to determine their agencies' overall effectiveness rating and the rating for each of the Cybersecurity Framework functions at the maturity level of their choosing. Using this approach, an IG may determine that a particular function area and the

[51] As previously stated in the report, OMB's responsibility in overseeing federal information security programs does not extend to national security systems.

agency’s information security program are effective at maturity levels lower than Level 4 (Managed and Measurable). According to both fiscal year 2020 and 2021 IG FISMA metrics guidance, the rationale for this is to provide greater flexibility so that the IGs may consider agency-specific factors such as mission, cybersecurity challenges, and resources. Further, the guidance did not detail when an IG should rely on the OMB threshold to determine agency ratings and when an IG should use an alternative methodology.

Consequently, the IG FISMA metrics guidance was not clear on when or how to apply the flexibilities and did not ensure consistent security program ratings. The flexibility allowed by the guidance introduced inconsistency into the IG rating process, as IGs could rate agencies as effective even if the assessment results suggested an ineffective rating. In addition, without additional clarity regarding when IGs should use their discretion with the ratings, the application of that flexibility will also be inconsistent.

The fiscal year 2020 IG ratings illustrate the inconsistencies allowed by the IG FISMA metrics guidance. For example, although the agencies did not reach OMB’s threshold for overall effectiveness, the Energy, DHS, and EPA IGs determined that their agencies had effective agency-wide information security programs in fiscal year 2020.[52] Rather, the IGs considered alternative input such as other IG work outside the FISMA metrics or used an alternative methodology to calculate ratings. Specifically:

- **Energy received a Level 4 (Managed and Measurable) rating in only one function and Level 3 (Consistently Implemented) ratings in each of the remaining four functions.** According to an Energy IG official, the department received an effective rating because the Energy IG’s fiscal year 2020 reviews did not indicate any systemic issues with the department’s information security programs. The official explained that the IG considers the totality of their work when making conclusions on overall effectiveness instead of solely basing the rating on the department’s performance against the FISMA metrics.

[52] Of the seven agencies with effective security programs in fiscal year 2020, four—GSA, NSF, NRC, and USAID—had IG ratings that met OMB’s threshold for overall effectiveness. Specifically, their IGs rated at least three of their core security functions at a Level 4 (Managed and Measurable) or higher.

- **DHS received two Level 4 (Managed and Measurable) ratings, two Level 3 (Consistently Implemented) ratings, and one Level 1 (Ad Hoc) rating.** DHS IG's independent assessment in the OMB Fiscal Year 2020 FISMA Annual Report to Congress states that the department's information security program was effective because it earned a maturity rating of Level 4 (Managed and Measurable) in three of the five core security functions. The information, however, is not consistent with the published maturity ratings in the same document, which show that DHS scored a Level 4 (Managed and Measurable) in only two functions. According to a DHS IG official, the IG based its final overall effective rating on maturity levels calculated by the raw metrics scores rather than the final risk-based IG assessments published in the OMB report.
- **EPA received Level 3 (Consistently Implemented) ratings in all five core security function ratings**. According to an EPA IG official, the agency received an effective rating because the IG concluded that EPA's information security program was effective at Level 3 (Consistently Implemented). Even though there are five maturity levels, the IG official informed us that the IG did not test for implementation beyond Level 3 (Consistently Implemented).

While the three agencies' effective ratings are in line with the flexibility that OMB's guidance allows, the different rationales illustrate how the various IG rating decisions and methodologies lead to final effectiveness ratings that are not easily comparable with the ratings of other agencies across the government. Further, the IGs for nine of the 16 civilian CFO Act agencies that did not receive effective ratings in fiscal year 2020 explicitly cited their use of OMB's recommended threshold for determining their agencies' overall ratings.[53] While these nine IGs might have had the same rating using the flexibility, the lack of clear guidance on the ratings does not provide assurance that ratings are consistent. As mentioned earlier, agencies also showed concern about the inconsistency of IG ratings and the effect of differences on agencies' FISMA evaluations.

Nevertheless, officials within CIGIE's Technology Committee stated that specifying the various instances where an IG could use an alternative methodology would cause FISMA evaluations to become more compliance-focused and less risk-based. Rather, the officials referred to

[53] The IGs' independent assessments for fiscal year 2020, in which agency IGs often justify their overall information security program rating, are found in OMB's fiscal year 2020 FISMA report to Congress. See Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2020 (Washington, D.C.: May 21, 2021).

OMB guidance, saying that agencies should perform a risk assessment and determine the optimal maturity level, and then OIGs should include that in their evaluation. That said, rather than creating an alternative methodology or moving away from risk-based processes, clarifying or creating additional guidance could encourage consistent ratings across the government.

According to the fiscal year 2021 IG FISMA reporting metrics, one of the goals of OMB's methodology is to ensure consistency in IG FISMA evaluations across the federal government. Despite this goal, the flexibility built into the guidance introduced increased inconsistency in the IGs' overall effectiveness ratings. Because of this inconsistency, the FISMA reporting process is not adequately providing a way to compare the performance of federal agencies' information security programs across the government. By updating the IG metrics guidance to include clearer instructions on when and how IGs should use flexibilities when making rating decisions, OMB would help IGs provide a more consistent picture of agencies' cybersecurity performance. Increased consistency may also give agency officials more confidence in how their agencies' effectiveness ratings compare to those determined by other agency IGs. Further, more consistent effectiveness ratings would enable Congress to better understand agencies' relative cybersecurity risks, thereby helping to improve the oversight of agencies' information security programs.

## OMB's Binary Effectiveness Scale Results in Imprecise IG Ratings

As previously mentioned, FISMA requires agency IGs to perform annual independent evaluations to determine and report on the effectiveness of their respective agency's information security program. OMB's annual IG metrics guide how the IGs perform these required assessments and make determinations on program effectiveness.

Specifically, OMB requires that IGs assess their agencies against a five-level maturity model and report an overall rating of effective or not effective. The current maturity model deems function areas and programs rated at any of the three lowest maturity levels as not effective. This means that, if an IG follows OMB's suggested rating process, an agency with consistently implemented policies, procedures, and strategies would have the same overall rating as an agency that performed security activities in an ad hoc, reactive manner.

Due to the significant differences between a program with a Level 3 (Consistently Implemented) maturity level and one at Level 1 (Ad Hoc), the not effective rating is imprecise and does not clearly communicate the effectiveness of an information security program. For example, as shown in table 4 above, agencies receiving not effective ratings in fiscal year 2020 had a wide range of maturity model ratings across the five core security functions. At the high end of the spectrum, Justice, Labor, and Interior all had three Level 3 (Consistently Implemented) ratings and two Level 4 (Managed and Measurable) ratings. If their respective IGs followed OMB's suggested rating process, all three agencies needed one more Level 4 (Managed and Measurable) rating to be assessed as having effective information security programs. In contrast, OPM had one Level 1 (Ad Hoc) rating, two Level 2 (Defined) ratings, one Level 3 (Consistently Implemented) rating, and one Level 4 (Managed and Measurable) rating. In comparison with the three previously mentioned agencies, OPM's scores are considerably lower, but also considerably more varied across the maturity model spectrum. The not effective rating assigned to all four agencies shows the limitations of the binary scale—specifically, that the scale is not able to adequately distinguish the differing levels of agencies' implementation of cybersecurity requirements, particularly for those agencies with lower program maturity.

These observations reflect the feedback on the ratings scale that we received from agency officials and officials from CISA. For instance, in support of the agency officials' suggestion to develop a gradient rating scale, CISA officials stated that the effective/not effective binary rating did not adequately communicate the status of an information security program's effectiveness, particularly concerning those agencies that receive a not effective rating.

Consequently, OMB's guidance does not support clear, sufficiently nuanced overall ratings that adequately reflect the effectiveness of agencies' information security programs. This lack of clarity limits the usefulness of the overall ratings to oversight bodies, as two agencies with not effective ratings could have significantly different levels of risk and security protection, as well as have significantly different needs in terms of resources and support. A more accurate scale with graduated ratings would help agencies to better compare their performance against other agencies and help Congress and other oversight bodies to focus their efforts and resources on the most critical programs.

## Conclusions

The recent SolarWinds breach underscores the importance of agencies addressing cybersecurity threats by improving their information security programs. However, federal agencies continued to have deficiencies in implementing information security programs and practices, and IGs at 16 of the 23 civilian CFO Act agencies rated their agencies' overall security program as not effective. To improve agencies' cybersecurity posture, we have made recommendations to address issues in areas such as risk management, cloud computing, vulnerability management, continuous network monitoring, and the security of information shared with third-party providers. Implementing these recommendations will strengthen information security programs and practices.

CIOs and CISOs at all 24 CFO Act agencies believe that FISMA has improved their information security programs to either a great or a moderate extent. In light of both the benefits of FISMA and impediments to its implementation, some of the IT officials' suggestions are being considered to improve the FISMA reporting process, including shifting the emphasis of FISMA reporting away from compliance and increasing the use of automation.

The agencies' suggestions to improve the FISMA reporting process include concerns about the consistency of IG FISMA ratings across the government. OMB provided IGs with guidance for rating their agencies, but this guidance introduced inconsistency into the rating process by not defining the conditions under which the IGs were to follow OMB's recommended methodology or, alternatively, use a different method to calculate agencies' overall effectiveness ratings. Further, the binary effective/not effective rating scale is vague and does not adequately reflect the actual risk facing an information security program, particularly for agencies receiving not effective ratings. Updating its IG ratings guidance to address these issues could help OMB ensure that future ratings present a more consistent and accurate picture of agencies' cybersecurity performance and could help oversight bodies to better understand the effectiveness of federal agencies' cybersecurity programs.

## Recommendations for Executive Action

We are making the following two recommendations to OMB:

The Director of OMB should collaborate with its partners in DHS and CIGIE to clarify the IG FISMA metrics guidance to specify when IGs should use OMB's recommended methodology and when they should use another method to determine agencies' overall effectiveness ratings. (Recommendation 1)

The Director of OMB should collaborate with its partners in DHS and CIGIE to create a more precise overall effectiveness rating scale for IG FISMA reports. (Recommendation 2)

## Agency Comments and Our Evaluation

We provided a draft of this report to OMB, the 24 CFO Act agencies, and CIGIE for review and comment. OMB, the one agency to which we made recommendations, did not concur with our recommendations. Of the 24 CFO Act agencies, five agencies agreed with our findings, two agencies neither agreed nor disagreed with our findings, and 17 agencies had no comments on the report. CIGIE did not state whether they agreed or disagreed with our findings. DOD, Education, DHS, and CIGIE provided technical comments, which we incorporated as appropriate.

Staff from OMB's Office of the Federal CIO responded to our draft via email and did not concur with either recommendation. Regarding our first recommendation to clarify the IG FISMA metrics guidance, OMB stated that its guidance establishes a foundational set of standards for IG audits while giving IGs the freedom to expand or adapt their reviews based upon their agencies' unique missions, resources, and challenges. OMB also noted that the implementation of this recommendation would add unnecessary complexity to FISMA audit standards, as well as potentially limit the independence of IGs by prescribing the circumstances in which case-specific adaptation of a standard may be appropriate.

We acknowledge OMB's position; however, our recommendation does not make any specific suggestions that would restrict the IGs' freedom to expand or adapt their reviews. Further, our recommendation does not advocate for a change in rating methodology that would add unnecessary complexity. Similarly, our recommendation does not suggest changes to OMB's guidance that would limit the independence of IG reviews.

Rather than proposing that specific changes be made to the rating methodology, our recommendation is to clarify the guidance so that IGs have clearer instructions on when they should use their flexibilities when making rating decisions. By doing so, OMB would help IGs provide a more consistent picture of agencies' cybersecurity performance. Consequently, we believe that this recommendation is still warranted.

With regard to our second recommendation to create a more precise overall effectiveness rating scale, OMB stated that, while the five point grading scale can seem too high-level, adding additional layers to the scale would not provide a clearer picture of agency effectiveness. OMB also noted that the current evaluation criteria are sufficient for determining the effectiveness and maturity of agency information systems and programs.

We maintain that implementing our recommendation would provide greater clarity to the ratings by more accurately reflecting agencies' implementation of their security programs to both Congress and other oversight bodies. Further, our recommendation does not suggest that OMB make any adjustments to the five point maturity model scale. Rather, our recommendation is for OMB to develop a more precise overall effectiveness rating scale, which currently is a binary scale of either effective or not effective.

Concerning the sufficiency of the current criteria, we found that the aforementioned flexibility in determining the overall rating introduced inconsistencies into the IG rating processes. Accordingly, IGs could rate agencies as effective even if the assessment results suggested an ineffective rating. In addition, the current binary rating scale does not allow the oversight bodies to adequately distinguish the differing levels of agencies' implementation of cybersecurity requirements, particularly for those agencies with lower program maturity. Consequently, we believe that the recommendation is warranted.

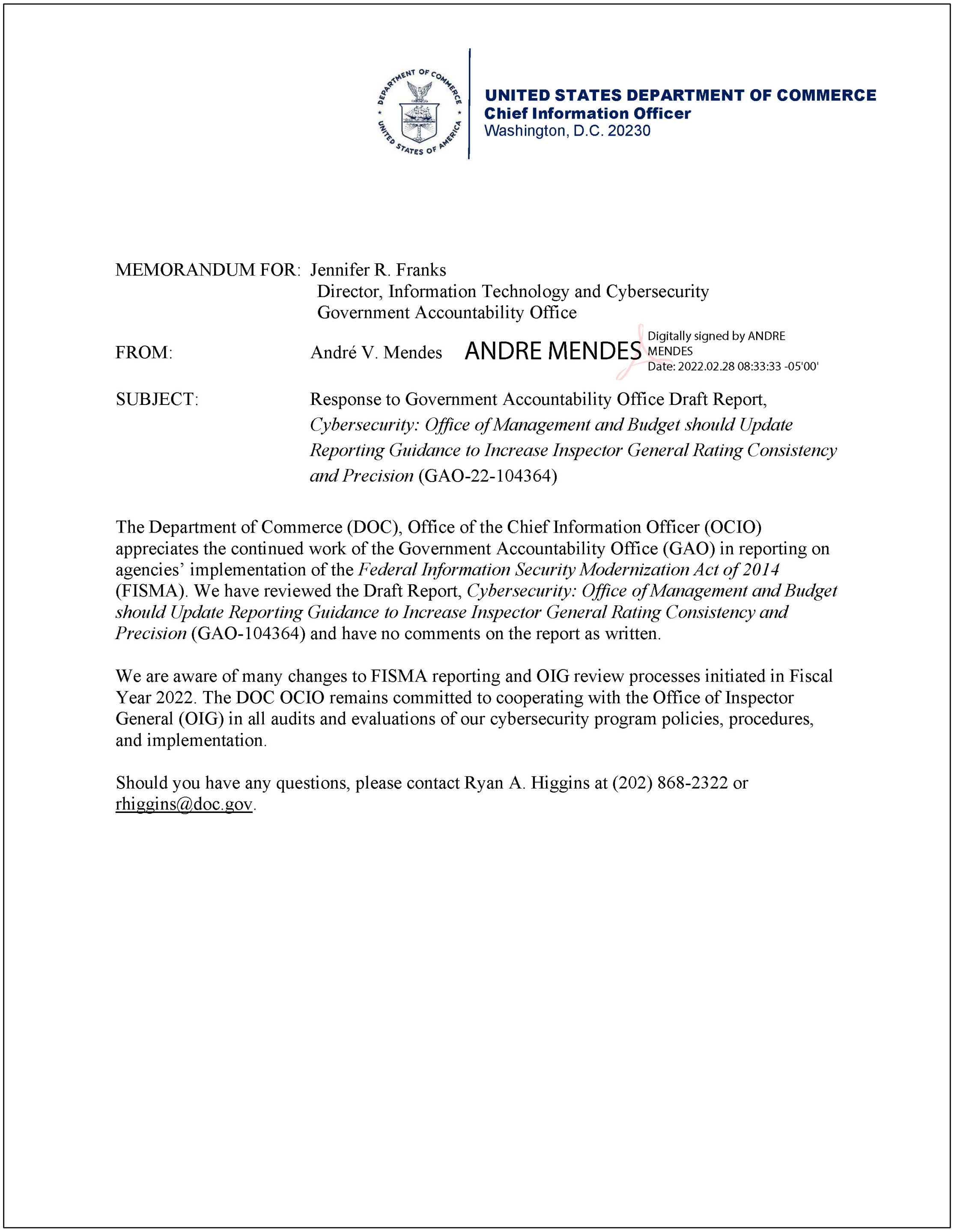
In addition to OMB, we received written comments from four agencies to which we did not make recommendations: Commerce, VA, SSA, and USAID. Commerce stated that it appreciated our continued FISMA reporting, but did not have any comments on the report. VA's written comments stated that the department generally concurred with the information and findings in our report. SSA and USAID expressed appreciation for the opportunity to review the report, but did not state whether they agreed or disagreed with our findings. These agencies' comments are reprinted in appendixes I-IV, respectively. The 20 remaining agencies that did not receive recommendations submitted their responses via email. Of the agencies that responded via email, four agreed with our findings, and 16 stated that they did not have comments on the report. We also received an email response from CIGIE containing technical comments that did not explicitly state whether they agreed or disagreed with our findings. As previously mentioned, we incorporated CIGIE's comments into the draft as appropriate.

We are sending copies of this report to the appropriate congressional committees, the heads of the 24 CFO Act agencies, and the Director of OMB. In addition, the report is available at no change on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (404) 679-1831 or FranksJ@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 V.

Jennifer R. Franks
Director, Information Technology and Cybersecurity

# Appendix I: Comments from the Department of Commerce



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

MEMORANDUM FOR: Jennifer R. Franks
Director, Information Technology and Cybersecurity
Government Accountability Office

FROM: André V. Mendes ANDRE MENDES Digitally signed by ANDRE MENDES
Date: 2022.02.28 08:33:33 -05'00'

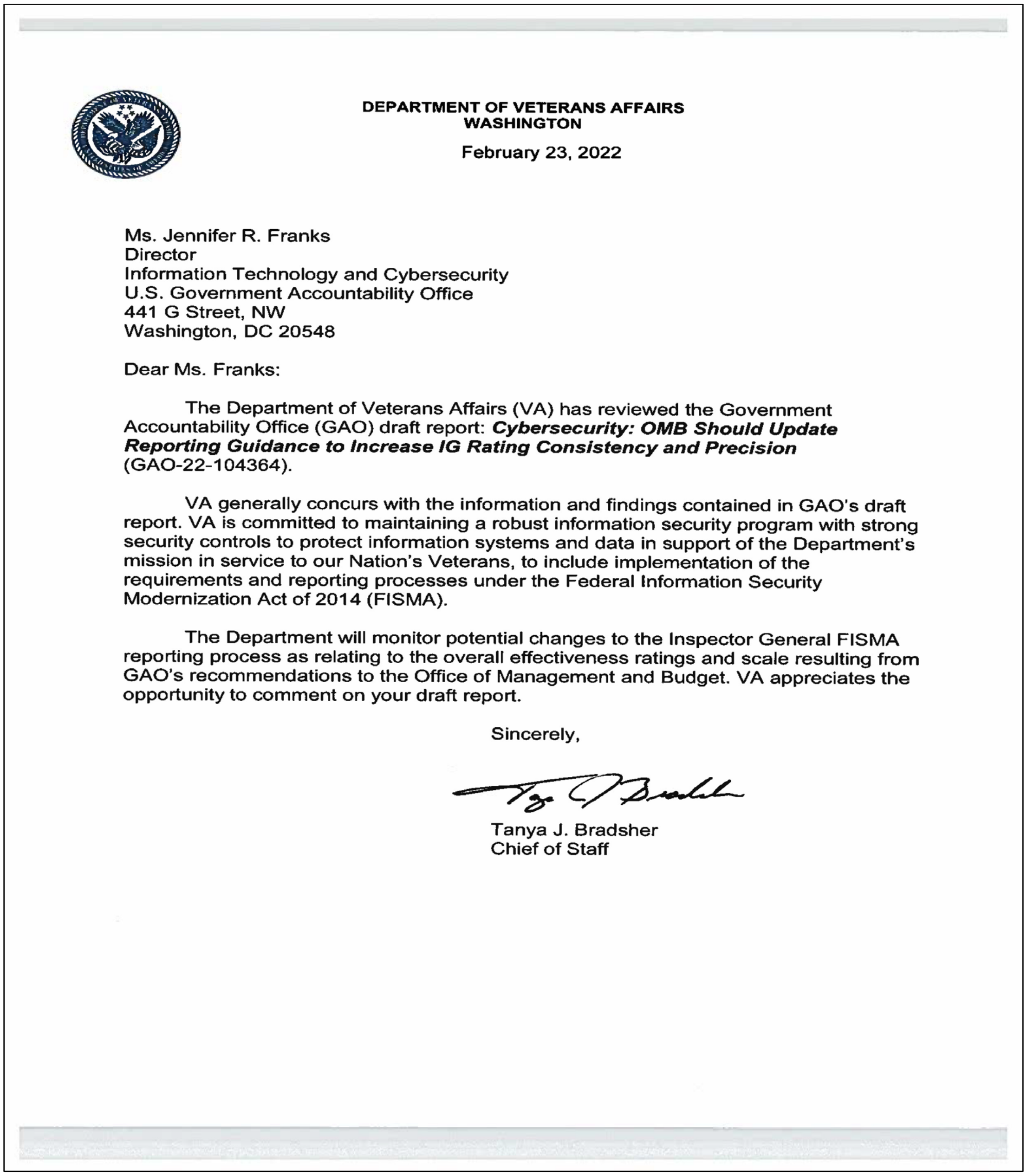
SUBJECT: Response to Government Accountability Office Draft Report, *Cybersecurity: Office of Management and Budget should Update Reporting Guidance to Increase Inspector General Rating Consistency and Precision* (GAO-22-104364)

The Department of Commerce (DOC), Office of the Chief Information Officer (OCIO) appreciates the continued work of the Government Accountability Office (GAO) in reporting on agencies' implementation of the *Federal Information Security Modernization Act of 2014* (FISMA). We have reviewed the Draft Report, *Cybersecurity: Office of Management and Budget should Update Reporting Guidance to Increase Inspector General Rating Consistency and Precision* (GAO-104364) and have no comments on the report as written.

We are aware of many changes to FISMA reporting and OIG review processes initiated in Fiscal Year 2022. The DOC OCIO remains committed to cooperating with the Office of Inspector General (OIG) in all audits and evaluations of our cybersecurity program policies, procedures, and implementation.

Should you have any questions, please contact Ryan A. Higgins at (202) 868-2322 or rhiggins@doc.gov.

# Appendix II: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

February 23, 2022

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***Cybersecurity: OMB Should Update Reporting Guidance to Increase IG Rating Consistency and Precision*** (GAO-22-104364).

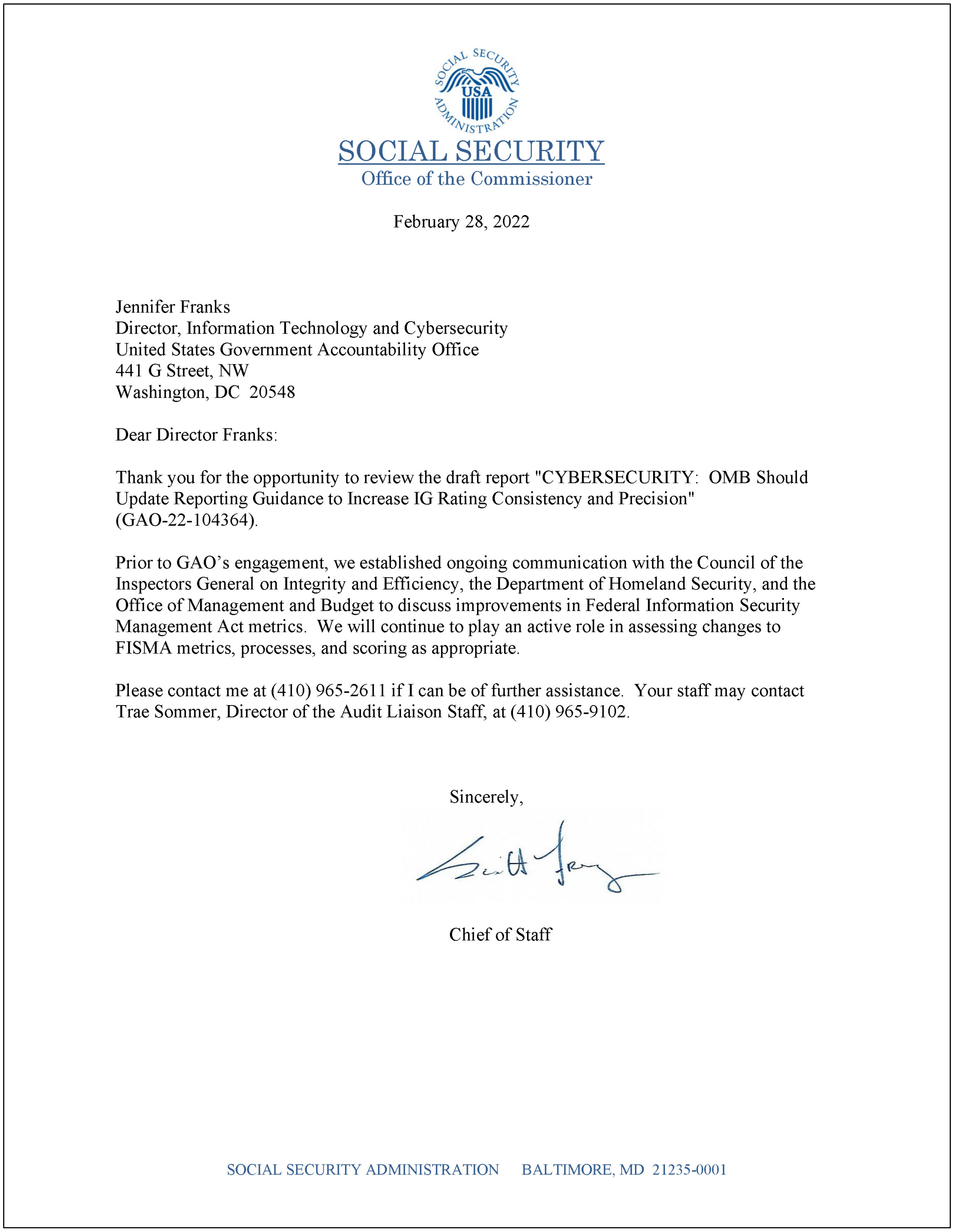
VA generally concurs with the information and findings contained in GAO's draft report. VA is committed to maintaining a robust information security program with strong security controls to protect information systems and data in support of the Department's mission in service to our Nation's Veterans, to include implementation of the requirements and reporting processes under the Federal Information Security Modernization Act of 2014 (FISMA).

The Department will monitor potential changes to the Inspector General FISMA reporting process as relating to the overall effectiveness ratings and scale resulting from GAO's recommendations to the Office of Management and Budget. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Tanya J. Bradsher
Chief of Staff

# Appendix III: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

February 28, 2022

Jennifer Franks
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC  20548

Dear Director Franks:

Thank you for the opportunity to review the draft report "CYBERSECURITY:  OMB Should Update Reporting Guidance to Increase IG Rating Consistency and Precision" (GAO-22-104364).

Prior to GAO's engagement, we established ongoing communication with the Council of the Inspectors General on Integrity and Efficiency, the Department of Homeland Security, and the Office of Management and Budget to discuss improvements in Federal Information Security Management Act metrics.  We will continue to play an active role in assessing changes to FISMA metrics, processes, and scoring as appropriate.

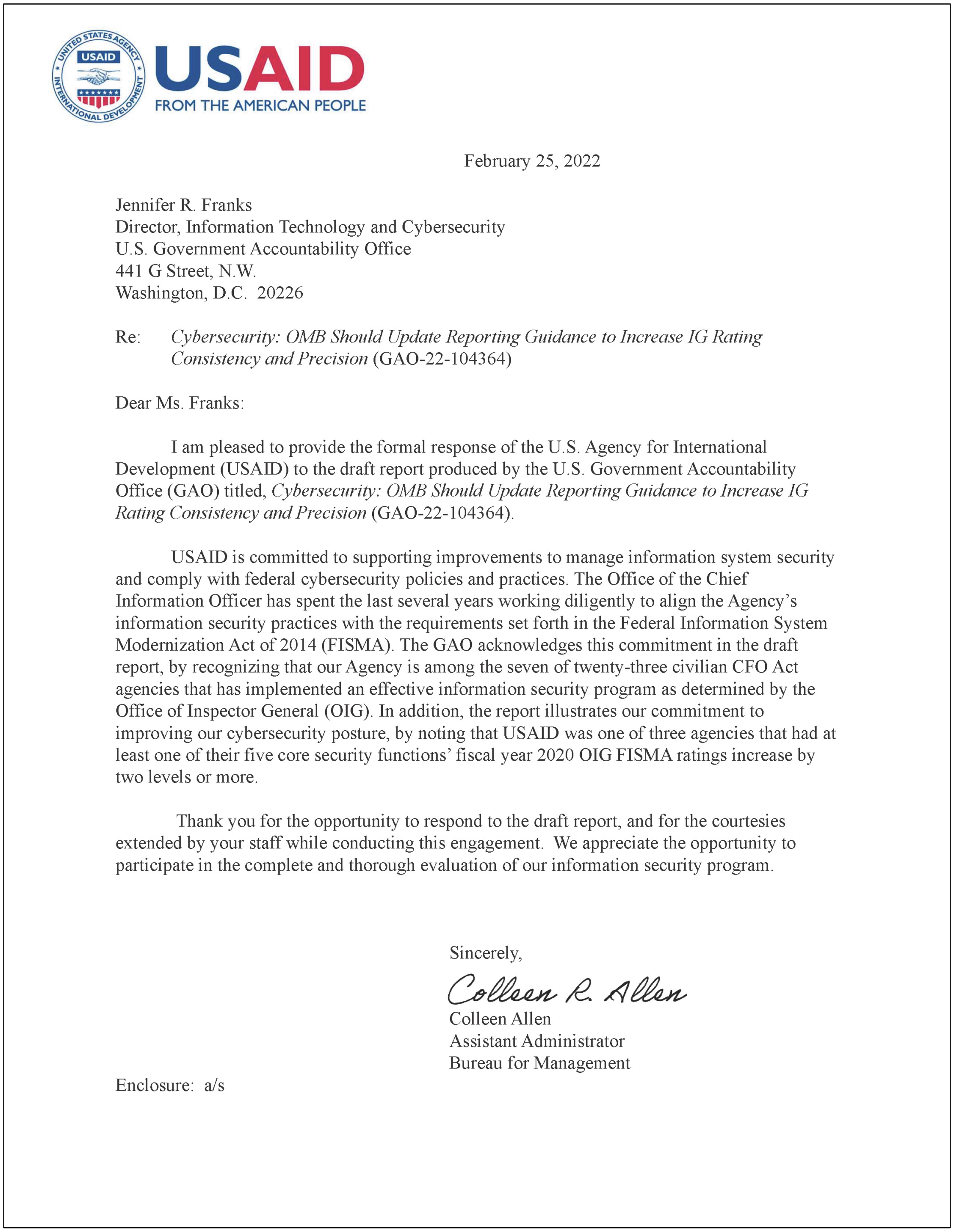
Please contact me at (410) 965-2611 if I can be of further assistance.  Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Chief of Staff

SOCIAL SECURITY ADMINISTRATION     BALTIMORE, MD  21235-0001

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



USAID
FROM THE AMERICAN PEOPLE

February 25, 2022

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: *Cybersecurity: OMB Should Update Reporting Guidance to Increase IG Rating Consistency and Precision* (GAO-22-104364)

Dear Ms. Franks:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *Cybersecurity: OMB Should Update Reporting Guidance to Increase IG Rating Consistency and Precision* (GAO-22-104364).

USAID is committed to supporting improvements to manage information system security and comply with federal cybersecurity policies and practices. The Office of the Chief Information Officer has spent the last several years working diligently to align the Agency's information security practices with the requirements set forth in the Federal Information System Modernization Act of 2014 (FISMA). The GAO acknowledges this commitment in the draft report, by recognizing that our Agency is among the seven of twenty-three civilian CFO Act agencies that has implemented an effective information security program as determined by the Office of Inspector General (OIG). In addition, the report illustrates our commitment to improving our cybersecurity posture, by noting that USAID was one of three agencies that had at least one of their five core security functions' fiscal year 2020 OIG FISMA ratings increase by two levels or more.

Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our information security program.

Sincerely,

Colleen R. Allen

Colleen Allen
Assistant Administrator
Bureau for Management

Enclosure: a/s

# Appendix V: GAO Contact and Staff Acknowledgments

## GAO Contact

Jennifer R. Franks, (404) 679-1831 or FranksJ@gao.gov

## Staff Acknowledgments

In addition to the contact named above, Vijay D'Souza (former Director), Larry Crosland (Assistant Director), Meredith Raymond (Analyst in Charge), Alina Budhathoki, Chris Businsky, Irene Li, Andrew Stavisky, and Edward Varty made key contributions to this report.

(104364)

## 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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

### 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 Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

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

## Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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