United States Government Accountability Office
Testimony
Before the Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 10: 00a.m. ET
Tuesday, January 11, 2022

CYBERSECURITY

Preliminary Results Show that Agencies' Implementation of FISMA Requirements Was Inconsistent

Statement of Jennifer R. Franks, Director,
Information Technology and Cybersecurity

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-22-105637

Chairwoman Maloney, Ranking Member Comer, and Members of the Committee:

Thank you for the opportunity to contribute to today's discussion on the *Federal Information Security Modernization Act of 2014* (FISMA).[1] As you know, 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 access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. Since 1997, GAO has designated information security as a government-wide high-risk area—a designation that it retains today.[2]

At your request, my remarks today will focus on our previous work, as well as key preliminary results from our ongoing review and a related draft report that evaluates the implementation of FISMA at agencies. Specifically, the draft report includes objectives intended 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. We anticipate sending the draft report to agencies for comment later this month.

[1]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 L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[2]See GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997); *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021). In 2003, we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.

For the first objective of that draft report, we reviewed 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; the Office of Management and Budget's (OMB) annual FISMA reports to Congress for fiscal years 2017 through 2020; and the annual FISMA assessments issued by the 23 agencies' inspectors general (IG) for fiscal years 2017 through 2020.[3] We also reviewed our reports on federal cybersecurity issued since December 2018.

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 chief information officers (CIO) and chief information security officers (CISO) at the 24 CFO Act agencies (i.e., the 23 civilian CFO Act agencies and the Department of Defense [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.

The work upon which this testimony is based is being conducted 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

FISMA was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information

[3]The 24 CFO Act agencies include DOD. However, DOD is not included in this section of the report due to data sensitivity concerns. The other 23 CFO Act agencies are Departments of Agriculture, Commerce, 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.

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 operations and assets of the agency. FISMA also requires agencies to comply with the Office of Management and Budget's (OMB) policies and procedures, Department of Homeland Security's (DHS) binding operational directives,[4] and National Institute of Standards and Technology's (NIST) federal information standards and guidelines.[5]

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.[6] 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,

[4]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.

[5]In working with OMB to develop these standards and guidelines, NIST is 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.

[6]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).

disclosure, disruption, modification, or destruction of agencies' information or information systems.

The act requires agencies to report annually to OMB, DHS, certain congressional committees, and GAO's 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. It also includes a provision for GAO to periodically report to Congress on agencies' implementation of the act.

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

FISMA requires agency IGs to annually assess the effectiveness of the information security policies, procedures, and practices of their parent agency.[7] 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 the Council of the Inspectors General on Integrity and Efficiency, in collaboration with other stakeholders. The fiscal year 2020 FISMA metrics guidance required IGs to conclude whether their agency's information security program was effective or not effective. Although guidance encouraged them to use the maturity model, they had discretion to consider agency-specific factors such as mission, cybersecurity challenges, and resources when determining a rating.

Federal Agencies Continued to Report a Large Number of Incidents in Fiscal Year 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 the DHS. 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

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

reported 30,819 incidents in fiscal year 2020—2,238 incidents higher than reported in fiscal year 2019.

FISMA also requires agencies to report and provide a description of any major security incident that occurs.[8] In its fiscal year 2020 report to Congress, OMB summarized the following six major incidents:[9]

- In September 2020, DOD reported a major incident in which a data analyst mistakenly sent an incorrect dataset to a Navy civilian employee through a secure file transfer application. The dataset involved personally identifiable information (PII)—including names, Social Security numbers, dates of birth, home addresses, personnel information, gender, and race. 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. 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 one vendor had applicable cybersecurity and privacy clauses for proper system access. 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. 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

[8]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.

[9]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).

dates, Social Security numbers, and alien numbers of current and former prisoners was stolen. 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, email addresses—and several other non-PII elements were erroneously sent to a vendor. An estimated 307,000 individuals were potentially affected.

Another incident that affected multiple federal agencies was the cybersecurity breach of the SolarWinds Orion software. In December 2020, CISA issued an emergency directive and alert explaining that an advanced persistent threat actor had compromised the supply chain of the network management software suite and inserted a "back door"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product. The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies and private sector organizations. We are conducting a comprehensive review of this breach, which we plan to complete in January 2022.

Preliminary Results Show Agencies' Uneven Effectiveness in Implementing Cybersecurity Requirements

Our preliminary results show that in fiscal year 2020, the 23 civilian CFO Act agencies reported progress toward meeting federal cybersecurity targets; nevertheless, a majority of the agencies reported not fully meeting the targets. In addition, IGs rated the majority of these 23 agencies as having ineffective IT security programs. Further, in our recent reports, 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 Federal Cybersecurity Targets

As part of their FISMA reporting for fiscal year 2020, agencies were to inform oversight bodies of their progress in meeting 10 cybersecurity targets by mitigating the risk and impact of threats to federal agencies' data, systems, and networks by implementing cutting edge cybersecurity

capabilities.[10] 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 federal cybersecurity targets. 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. For example:

- In 2020, 18 agencies reported meeting targets related to **intrusion detection and prevention**. Specifically, the 18 agencies reported that they had implemented at least four of six intrusion prevention metrics at an implementation target of at least 90 percent and analyzed 100 percent of email traffic using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source. This was an increase from 2018, in which seven agencies reported that they had met targets related to intrusion detection and prevention.
- In 2020, 19 agencies reported meeting the target related to **automated access management**. Specifically, the 19 agencies reported that 95 percent of their users were covered by an automated, dynamic access management solution that centrally tracked access and privilege levels. This was an increase from 2018, in which 15 agencies reported that they had met a target related to automated access management.

However, even with these increases, 17 of the 23 agencies did not meet all 10 of the federal cybersecurity targets in fiscal year 2020.

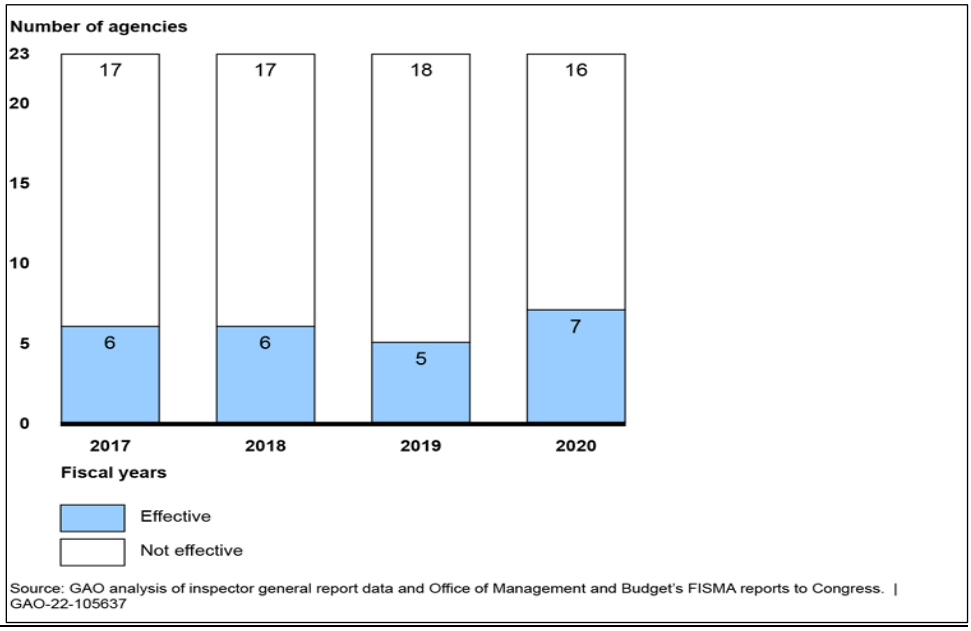
Inspectors General Rated Seven of 23 Agencies as Having Effective IT Security Programs in Fiscal Year 2020

IGs determine whether or not their agencies' IT security programs are effective or not. In their fiscal year 2020 FISMA reports, IGs concluded that seven of the 23 civilian CFO Act agencies had effective information security programs. The total number of civilian CFO Act agencies receiving effective ratings has remained fairly consistent over the four most recent annual assessments. In addition to the total number of agencies receiving effective ratings remaining relatively constant, the specific agencies receiving those effective ratings has also remained

[10]The 10 targets are intended to address a variety of cybersecurity topics associated with software asset management, hardware asset management, authorization management, mobile device management, privileged network access management, high-value asset access management, automated access management, intrusion detection and prevention, exfiltration and enhanced defenses, and data protection.

relatively constant with a slight increase in effective programs in fiscal year 2020. Figure 1 shows the number of the 23 agencies that IGs rated as effective and ineffective between fiscal years 2017 and 2020.

Figure 1: Number of 23 Civilian *Chief Financial Officers Act of 1990* Agencies with 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 FISMA reports to Congress. | GAO-22-105637

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

GAO has also routinely reported on agencies' inconsistent implementation of federal cybersecurity policies and practices. Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings, of which about 900 were not yet fully implemented as of November 2021. In addition, in March 2021, we reported that federal agencies need to take urgent actions to, among other things, secure federal systems and protect cyber critical infrastructure, privacy, and sensitive data.[11]

Further, our recent reviews have identified cybersecurity weaknesses at various agencies, including the Internal Revenue Service (IRS), Department of Housing and Urban Development (HUD), DOD, and

[11]GAO-21-229SP

Centers for Disease Control and Prevention (CDC). Consequently, we made recommendations to these agencies.

- **IRS:** In May 2021, we reported on the information system security controls of IRS processing and management systems.[12] In the report, we highlighted newly identified and continuing deficiencies related to access controls and configuration management. For example, we noted that IRS did not always remove certain accounts and users in accordance with agency policy.

  We made five new recommendations to improve IRS's cybersecurity. In addition, IRS had 91 recommendations that it had not yet fully-implemented from prior year audits. We will continue to follow-up on the implementation of our recommendations as part of our annual financial statement audit at IRS.

- **HUD**: 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. In September 2020, we reported that HUD was not effectively protecting sensitive information exchanged with external entities.[13] 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 December 2021, HUD had not implemented any of the five recommendations.

[12]GAO, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls,* GAO-21-401R (Washington, D.C.: May 4, 2021).

[13]GAO, *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).

- **DOD:** 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.[14] 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.[15] However, DOD officials have stated that there is no commonly used definition for cyber hygiene in DOD doctrine.

  We also 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 or not providing complete status updates to senior leaders. Further, we noted that, while the department had created a Cyber Hygiene 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.[16]

  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 December 2021, DOD had not yet implemented any of the seven recommendations.

- **CDC:** 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

[14]GAO, *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene,* GAO-20-241 (Washington, D.C.: Apr. 13, 2020).

[15]*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 Committee),* 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).

[16]As part of its cyber hygiene initiative, DOD created a Cyber Hygiene Scorecard to measure compliance with DOD cybersecurity policies, procedures, standards, and guidelines.

issued in June 2018.[17] In that report, we had made 195 recommendations to strengthen CDC's technical security controls and bolster its agency-wide information security program.

CDC 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.

Preliminary Results Demonstrate That FISMA Improved Cybersecurity, but also Identified Impediments and Suggested Improvements

According to our preliminary results, officials such as CIOs and CISOs at each of the 23 civilian CFO Act agencies and DOD reported that 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.

Officials Reported That FISMA Enabled Agencies to Improve Their Cybersecurity Programs

The enactment of FISMA was to, among other things, provide a mechanism for improved oversight of agencies' information security programs, including through automated security tools to continuously diagnose and improve security. 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

[17]GAO, *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). 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.

their agencies to improve their security programs' effectiveness to a moderate extent.[18]

In responding to our interview questions, officials from all 24 CFO Act 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. Of the 24 CFO Act agencies, for example:

- **Standardized security program requirements.** Officials at 10 agencies stated that FISMA was effective because it standardized their security program requirements.
- **Mandated security requirements.** Officials at four agencies responded that FISMA's status as a legal requirement provided the authority to take actions that helped improve their cybersecurity posture.
- **Helped justify cybersecurity requests to management.** Officials at four agencies stated that FISMA had helped them make convincing cybersecurity requests to management.
- **Allowed for more effective communication within the agency.** Officials at four agencies discussed how FISMA had helped improve communication about cybersecurity issues within their agencies.
- **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.
- **Guided agency priorities and security efforts.** Officials at four agencies cited FISMA's ability to guide agency priorities and security efforts.
- **Established responsibilities and authorities related to the cybersecurity program.** Officials at four agencies stated that FISMA helped to establish cybersecurity responsibilities and authorities.

[18]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.

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. [19] Of the 24 CFO Act agencies, for example:

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

Agency Officials Suggested Ways to Improve the FISMA Reporting Process

Agency officials also provided a number of suggestions for improving the effectiveness of the FISMA metrics, annual evaluations, and reporting process. Of the 24 CFO Act agencies, for example:

- **Update the metrics to increase their effectiveness.** Officials at 11 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.

  Officials from DHS who help develop the metrics agreed with the agencies' suggestions to update the metrics, and stated that they work to annually update the metrics to address threats and vulnerabilities and to remove out-of-date metrics. The officials further stated that, during the annual update process, they obtain feedback about agencies' concerns via meetings and email.

[19]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.

- **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.

  In December 2021, OMB issued guidance that attempts to shift the emphasis of FISMA reporting away from compliance and in favor of risk management.[20] For example, the guidance encourages IGs to focus on the practical security impact of weak control implementation, 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 instead of manual data calls.

  OMB's December 2021 guidance emphasizes automation and the use of machine-readable data to speed up reporting, reduce the burden on agencies, and improve outcomes. The guidance further directs the development of a strategy to enable agencies to report performance and incident data in an automated, machine-readable manner.

- **Improve the IG evaluation process and the maturity-rating model.** Officials at eight agencies suggested making changes to the IG evaluation process and the maturity ratings. For example, 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.

  DHS officials stated that they were in favor of the suggestion to develop a gradient rating scale. Specifically, the officials stated that the effective/not effective binary rating did not adequately communicate the status of an information security program's effectiveness.

[20]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).

- **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.

  According to its December 2021 guidance, OMB will be implementing a new reporting cycle for the IG FISMA metrics. Specifically, the guidance 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 2-year cycle on a calendar agreed to by OMB and its partners.

In summary, while agencies have made some progress in improving their information security programs, inspectors general and GAO have identified shortcomings in agency implementation of federal cybersecurity requirements. Although agency officials have reported that FISMA has helped them improve their cybersecurity programs, they have also reported impediments to following FISMA, and suggestions for improving it. Until federal agencies are able to fully implement federal cybersecurity requirements, their systems and data will remain at heightened risk.

Chairwoman Maloney, Ranking Member Comer, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Jennifer R. Franks, Director of Information Technology and Cybersecurity, 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 statement. GAO staff who made key contributions to this testimony include Larry Crosland and Jeffrey Knott (Assistant Directors), Meredith Raymond and Kevin Smith (Analysts in Charge), Alina Budhathoki, Chris Businsky, Vijay D'Souza, Franklin Jackson, Irene Li, Ahsan Nasar, Priscilla Smith, Andrew Stavisky, Edward Varty, and Umesh Thakkar made key contributions to this report.