United States Government Accountability Office

Report to Congressional Committees

January 2024

CYBERSECURITY

OMB Should Improve Information Security Performance Metrics

Accessible Version

GAO-24-106291

GAO Highlights

Highlights of GAO-24-106291, a report to congressional committees

January 2024

CYBERSECURITY

OMB Should Improve Information Security Performance Metrics

Why GAO Did This Study

To protect federal information and systems, FISMA requires federal agencies to develop, document, and implement information security programs. FISMA includes a provision for GAO to periodically report on agencies' implementation of the act.

GAO's objectives in this report were to identify (1) the reported effectiveness of agencies' efforts to implement FISMA; (2) the key practices used by agencies to meet FISMA requirements; and (3) how FISMA metrics could be changed to better measure the effectiveness of federal agency information security programs.

To do so, GAO reviewed the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies' FISMA reports, agency reported performance data, and OMB documentation and guidance. The Department of Defense (DOD) was not included in GAO's analysis of performance data due to DOD's classification of the information. GAO also solicited perspectives from the 24 CFO Act agencies (including DOD) and interviewed officials with the Council of Inspectors General on Integrity and Efficiency, the Cybersecurity and Infrastructure Security Agency, and OMB.

What GAO Recommends

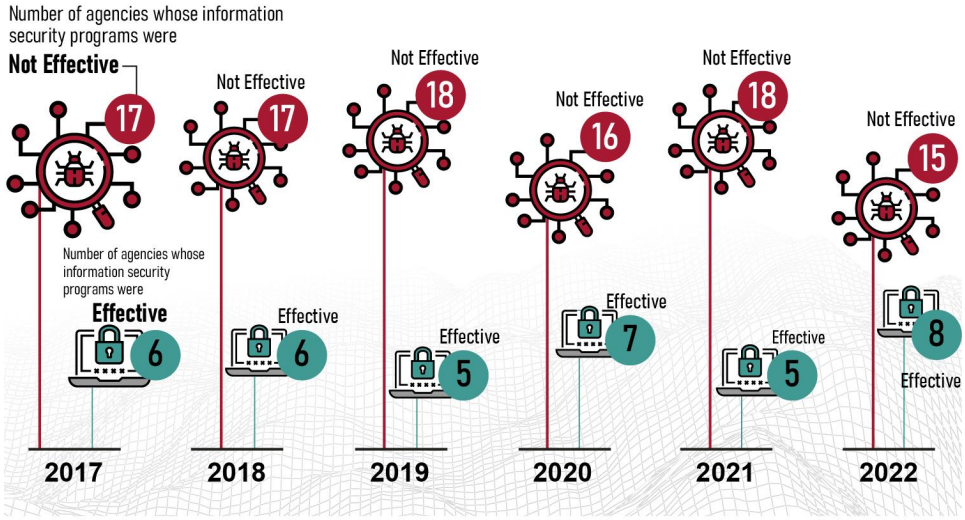
GAO is making two recommendations for OMB to collaborate with its partners to enhance FISMA metrics that can lead to more effective programs and performance. OMB neither agreed nor disagreed with the recommendations and provided technical comments that were incorporated as appropriate.

View GAO-24-106291. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

What GAO Found

Federal agencies' implementation of the Federal Information Security Modernization Act of 2014 (FISMA) continued to be mostly ineffective. Although some improvement was reported from 2021 to 2022, inspectors general (IG) of 15 of the 23 civilian agencies found the information security programs to be ineffective (see figure). IGs reported various causes for the ineffective programs, including management accountability issues and gaps in standards and quality control. Addressing the causes could improve the federal government's cybersecurity posture.

23 Chief Financial Officers Act of 1990 Agencies That Do or Do Not Have Effective Information Security Programs, as Reported by Inspectors General, Fiscal Years 2017 through 2022.



Sources: GAO (analysis); civilian agencies subject to Chief Financial Officers Act of 1990 (data); PST Vector/stock.adobe.com (background); lovemask/stock.adobe.com (icons). | GAO-24-106291

Agency officials identified various practices that have contributed to improving the effectiveness of their agency's information security program. Specifically, officials most often highlighted internal communication; organizational characteristics, such as leadership commitment; and centralized policies and procedures as being essential to effectively implement FISMA.

The Office of Management and Budget (OMB), in collaboration with other oversight groups, provides metrics to evaluate the effectiveness of federal information security programs and implementation of FISMA. However, agencies and IGs stated that some FISMA metrics are not useful because they do not always accurately evaluate information security programs. Agencies and IGs reported that metrics should be clearly tied to performance goals, account for workforce issues and agency size, and incorporate risk. Further, crafting metrics that address the key causes of ineffective programs could enhance their effectiveness. By modifying FISMA metrics in these ways, OMB could help ensure that the measures provide an accurate picture of agencies' information security performance.

Contents

GAO Highlights ii

Letter 1

Background 4
CIOs and IGs Reported Varied Progress in Implementing FISMA 16
A Variety of Practices Contributed to Improvement in Information Security Programs' Effectiveness 27
Agencies Suggest That OMB Should Modify Metrics to Better Measure Information Security Effectiveness 33
Conclusions 41
Recommendations for Executive Action 42
Agency Comments 42

Appendix I: Objectives, Scope, and Methodology 44

Appendix II: Practices Highlighted by Agencies on FISMA Implementation 48

Appendix III: Comments from the Social Security Administration 55

Accessible Text for Appendix III: Comments from the Social Security Administration 56

Appendix IV: Comments from the U.S. Agency for International Development 57

Accessible Text for Appendix IV: Comments from the U.S. Agency for International Development 58

Appendix V: GAO Contact and Staff Acknowledgments 59

GAO Contact 59
Staff Acknowledgments 59

Tables

Table 1: Civilian Chief Financial Officers Act of 1990 (CFO Act) Agencies' Status of Fiscal Year 2022 Federal Information Security Modernization Act (FISMA) Chief Information Officer (CIO) Metrics Relevant to Administration Priorities 17
Table 2: Inspector General Evaluation Maturity Levels for Assessing Agencies' Information Security Programs 18
Table 3: Inspector General (IG) Maturity Level and Overall Ratings of the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Programs for Fiscal Year 202122

Table 4: Inspector General (IG) Maturity Level and Overall Ratings of the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Programs for Fiscal Year 202223
Table 5: Practices Highlighted by Department of Energy Officials That Contribute Positively to Information Security Program Effectiveness 48
Table 6: Practices Highlighted by Department of Justice Officials That Contribute Positively to Information Security Program Effectiveness 49
Table 7: Practices Highlighted by General Services Administration Officials That Contribute Positively to Information Security Program Effectiveness 51
Table 8: Practices Highlighted by National Science Foundation Officials That Contribute Positively to Information Security Program Effectiveness 53
Table 9: Practices Highlighted by Small Business Administration Officials That Contribute Positively to Information Security Program Effectiveness 54

Figures

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2017 through 2022 6
Accessible Data Table for Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2017 through 2022 6
Figure 2: Information Security Incidents Reported by Federal Agencies and Categorized by Threat Vector in Fiscal Year 2022 7
Figure 3: National Institute of Standards and Technology Cybersecurity Framework 11
Figure 4: Number of Civilian Agencies Subject to the Chief Financial Officers Act of 1990 That Do or Do Not Have Effective Information Security Programs, as Reported by Inspectors General, Fiscal Years 2017 through 2022 21
Figure 5: Perspectives from the 24 Chief Financial Officers Act of 1990 Agency Inspectors General on the Causes of Ineffective Information Security Programs 25
Accessible Data Table for Figure 5: Perspectives from the 24 Chief Financial Officers Act of 1990 Agency Inspectors

General on the Causes of Ineffective Information Security Programs 25
Figure 6: Causes of Program Ineffectiveness for the 23 civilian Chief Financial Officers Act of 1990 Agencies Reported by Inspectors General in Fiscal Year 2022 27
Figure 7: Practices Highlighted by Selected Agencies as Contributing to Higher Overall Federal Information Security Modernization Act of 2014 (FISMA) Maturity Ratings 29
Figure 8: Examples of Federal Agencies' Views on How FISMA Metrics Should Be Modified for Risk 38
Figure 9: Example of How Federal Information Security Modernization Act of 2014 (FISMA) Metrics May Not Provide an Accurate Picture of An Agency's Encryption Implementation 40

Abbreviations

CAP	Cross Agency Priority
CFO Act	Chief Financial Officers Act of 1990
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
DOD	Department of Defense
FISMA	Federal Information Security Modernization Act of 2014
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PII	personally identifiable information

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 9, 2023

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
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.

GAO first designated information security as a government-wide high-risk area in 1997.[1] Our high-risk designation emphasizes the need for the federal government to take actions 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.[2] Most recently, we continued to identify federal information security as a government-wide high-risk area in our April 2023 high-risk update.[3]

[1]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).

[2]GAO, *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, GAO-23-106415 (Washington, D.C.: Jan. 19, 2023). See also https://www.gao.gov/high-risk-list.

[3]GAO, *High- Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023).

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies in the executive branch to develop, document, and implement information security programs to protect the information and systems that support the agencies' operations and assets.[4] The act also requires agency Chief Information Officers (CIO) to submit FISMA reports on their information security programs to the Office of Management and Budget (OMB), Department of Homeland Security (DHS), GAO, and Congress. 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 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 identify: (1) the reported effectiveness of agencies' efforts to implement FISMA, (2) key practices used by agencies to meet FISMA requirements, and (3) how FISMA metrics could be changed to better measure the effectiveness of federal agency information security programs.

To address the first objective, we analyzed information from the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies' annual FISMA CIO and IG reports for the fiscal years 2021 and 2022.[5] We used

[4]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.

[5]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 report of agencies' performance data because the department has classified the information in its FISMA reports.

this analysis to develop an overview of the state of federal cybersecurity and a summary of government-wide FISMA implementation.

In addition, we reviewed IG FISMA reports to identify causes for ineffective information security program deficiencies. Further, we developed a questionnaire and administered it to all 24 CFO Act agencies to determine the extent to which certain common challenges were causes of ineffective information security programs.

To address the second objective, we solicited perspectives from five selected agencies on practices they implemented that have resulted in positive outcomes for their information security programs and implementation of FISMA.[6] For the selection, we considered agencies with a composite score totaling 15 or greater from their 2021 IG FISMA evaluations of the National Institute of Standards and Technology (NIST) Cybersecurity Framework functional areas (a score of 25 is the highest any one agency could achieve) as reported by OMB.[7] To obtain agency perspectives, we conducted semi-structured interviews with Office of the CIO, Office of the Chief Information Security Officer (CISO), and IG officials from selected civilian CFO Act agencies.

In addition, we analyzed documentary evidence of the cybersecurity practices discussed by agency officials. Further, we met with officials from each agency's IG to validate information from agency officials and gain their perspective on the practices identified by the agency.

To address the third objective, we identified and reviewed the CIO and IG FISMA metrics and guidance documentation. Further, we solicited the perspectives of each of the 24 CFO Act agency Offices of the CIO and IGs on the FISMA metrics. Specifically, we analyzed data collection instruments and questionnaires administered to agencies and their IGs regarding their opinions on the usefulness of each FISMA metric. We also interviewed officials from OMB, the Cybersecurity and Infrastructure

[6]The selected agencies are the Departments of Energy and Justice, the General Services Administration, the National Science Foundation, and the Small Business Administration.

[7]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2021* (Washington, D.C.: Sep. 14, 2022). Agencies and their IGs use the framework in reporting on the effectiveness of agency information security policies and practices and the implementation of FISMA. The metrics used for FISMA reporting correspond to the core functions outlined in the framework. The NIST Cybersecurity Framework is based on five core security functions—identify, protect, detect, respond, and recover. This report includes more detail on the framework in later sections.

Security Agency (CISA), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to discuss their role in developing FISMA metrics. For more details on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from October 2022 to January 2024 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. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can gain 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 emerge 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.

Reports of Cybersecurity Incidents Have Slightly Declined Over the Past Six Years

In its fiscal year 2022 report to Congress, OMB stated that 30,659 incidents were reported by civilian agencies in fiscal year 2022—a 5.7

percent decrease from fiscal year 2021. Three of these incidents were considered major.[8]

- The Department of Agriculture had a major process failure involving a breach of personally identifiable information (PII), including employee's full names, social security numbers, home addresses, and wages. This affected 69,708 individuals.
- The Department of Education experienced a breach involving PII through a vulnerability on a vendor-operated loan registration website. The system was shut down once the activity had been detected.
- The Department of the Treasury's Internal Revenue Service had a major incident involving a breach of PII from forms filed by tax-exempt entities, including names, addresses, email addresses, and phone numbers.

In addition, in fiscal year 2023, three noteworthy incidents affected federal government operations.

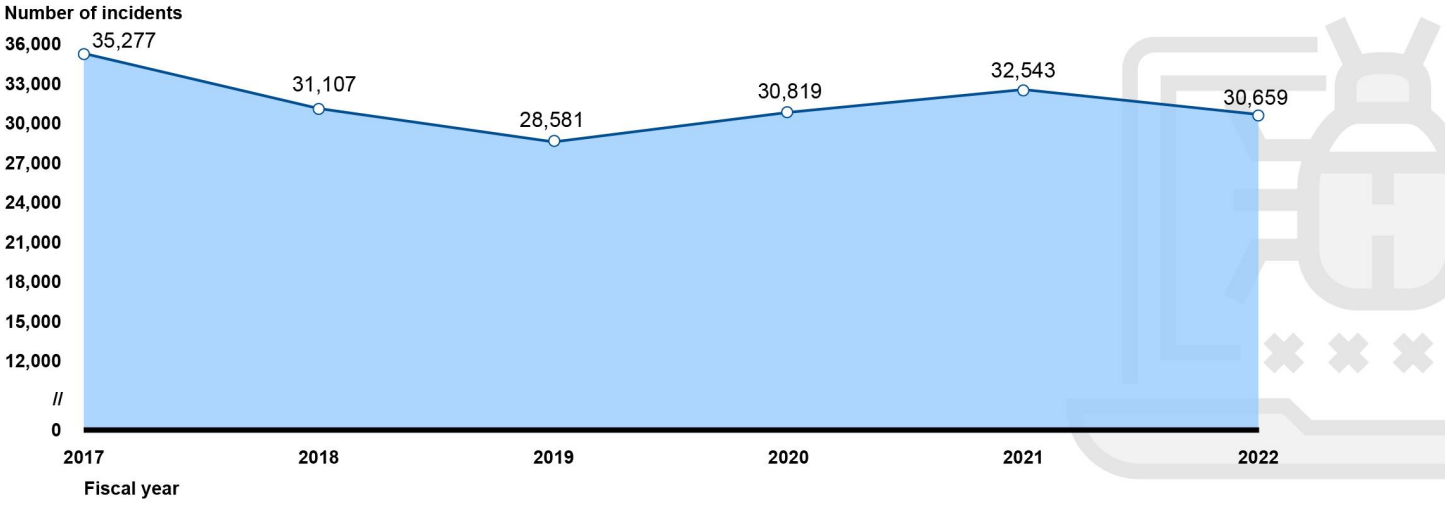
- On February 17, 2023, malicious actors breached a U.S. Marshals system using ransomware.[9] The system contained administrative information and PII.
- On May 27, 2023, Russian-linked hackers exploited a vulnerability, known as the MOVEit Transfer, on Department of Energy systems. The vulnerability allowed the malicious actors to potentially escalate privileges and gain unauthorized access to Energy systems.
- In June 2023, a China-based threat actor exploited a vulnerability in the Microsoft 365 environment that allowed them to impersonate users and gain access to enterprise emails at the Departments of State and Commerce.

[8]According to OMB, a major incident is either (1) an 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]Ransomware is a form of malicious software designed to render the underlying data and systems unusable. Ransom payments are then demanded in exchange for restoring access to the locked data and systems. For more information on ransomware, see GAO, *Ransomware: Federal Coordination and Assistance Challenges*, GAO-23-106279 (Washington, D.C.: Nov. 16, 2022).

Civilian agencies across the federal government are required to report their cybersecurity incidents to CISA, a component of DHS. Overall, the 6-year trend in number of incidents reported by federal agencies, shown in figure 1 below, showed a slight decline.

Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2017 through 2022



Sources: GAO (analysis); U.S. Computer Emergency Readiness Team and Office of Management and Budget (data); lovemask/stock.adobe.com (icon). | GAO-24-106291

Accessible Data Table for Figure 1: Federal Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team, Fiscal Years 2017 through 2022

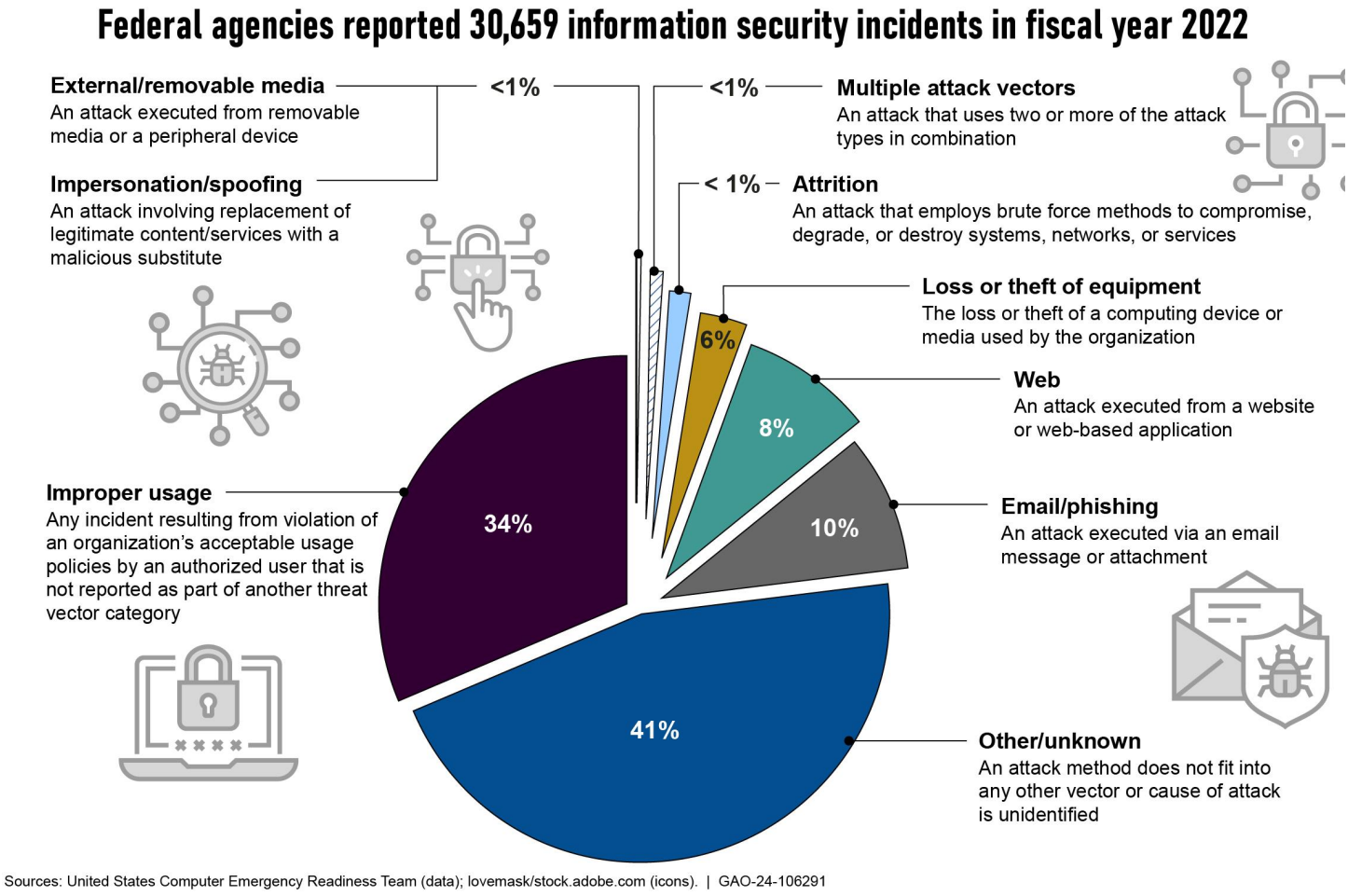
Fiscal Year	Number of Incidents
2017	35,277
2018	31,107
2019	28,581
2020	30,819
2021	32,543
2022	30,659

Sources: GAO (analysis): U.S. Computer Emergency Readiness Team and Office Management and Budget (data): lovemask/stock.adobe.com (icon) | GAO-24-106291

According to the United States Computer Emergency Readiness Team incident report data, the incidents reported in fiscal year 2022 involved several threat vectors, including improper usage of an authorized user, phishing attacks, web-based attacks, and the loss or theft of computer

equipment, among others.[10] Figure 2 provides a breakdown of the fiscal year 2022 information security incidents by threat vector.

Figure 2: Information Security Incidents Reported by Federal Agencies and Categorized by Threat Vector in Fiscal Year 2022



Sources: United States Computer Emergency Readiness Team (data); lovemask/stock.adobe.com (icons). | GAO-24-106291

For fiscal year 2022, the "other/unknown" vector accounted for the highest number of reported incidents. According to OMB's fiscal year 2022 report to Congress, the prevalence of this attack vector suggests additional rigor must be applied by agencies to appropriately categorize the vector of incidents during reporting, and when applicable, update the

[10]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack. Phishing is an email-based attack. A web-based attack is executed from a website or web-based application.

initial report when the vector is identified during the investigation process. To illustrate, our 2023 report on Department of Defense (DOD) cybersecurity found that the department did not include information on an incident's threat vector in 68 percent of their reported incidents.[11] This limited the department's ability to identify trends in the prevalence of various threats affecting its networks. We made six recommendations to improve information sharing, but as of September 2023 DOD had not implemented these recommendations.

"Improper usage" was the second most prevalent vector. In its fiscal year 2022 report to Congress, OMB stated that the data on these incidents suggest that although agencies have processes or capabilities that detect when a security policy is being violated, many lack automated enforcement or prevention mechanisms. Implementing these mechanisms could reduce the risk of improper usage incidents by preventing them before they happen.

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 resources that support federal operations and assets. The act addresses the increasing sophistication of cyberattacks, promotes the use of automated security tools that can continuously monitor and diagnose federal agencies' security posture, and provides for improved oversight of their information security programs.

FISMA requires agencies to develop, document, and implement an agency-wide program to secure federal information systems and data. These information security programs are to provide risk-based protections for the information and information systems that support the operations and assets of the agency. FISMA requires agencies to comply with OMB's policies and procedures, DHS's binding operational directives, and NIST's federal information standards and guidelines.[12]

[11]GAO, *DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared*, GAO-23-105084 (Washington, D.C.: Nov. 14, 2022).

[12]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.

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.[13] The act further assigns OMB the responsibility of requiring agencies to identify and provide information security protections. These protections are to be 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. They are to do this 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. Under DHS, CISA 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 required to consult with federal agencies and other organizations. These consultations are 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

[13]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).

effectiveness of the information security policies, procedures, and practices of their parent agency.[14] 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.[15]

Federal Agencies and IGs Use a Variety of Tools to Report on Effectiveness of FISMA Implementation

NIST, OMB, and others have developed a variety of tools that are to be used by federal agencies and their IGs to determine the extent to which FISMA requirements have been effectively implemented. Specifically, agencies use NIST's Cybersecurity Framework as a tool for reporting on the maturity of agency information security policies and practices and the implementation of FISMA.[16] In addition to NIST's Framework, OMB and CIGIE have developed performance metrics to measure FISMA implementation.[17]

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

In May 2017, Executive Order 13800 directed each executive branch agency to use the NIST Cybersecurity Framework to manage its

[14]For agencies without an Inspector General, the head of the agency shall engage an independent external auditor to perform the evaluation.

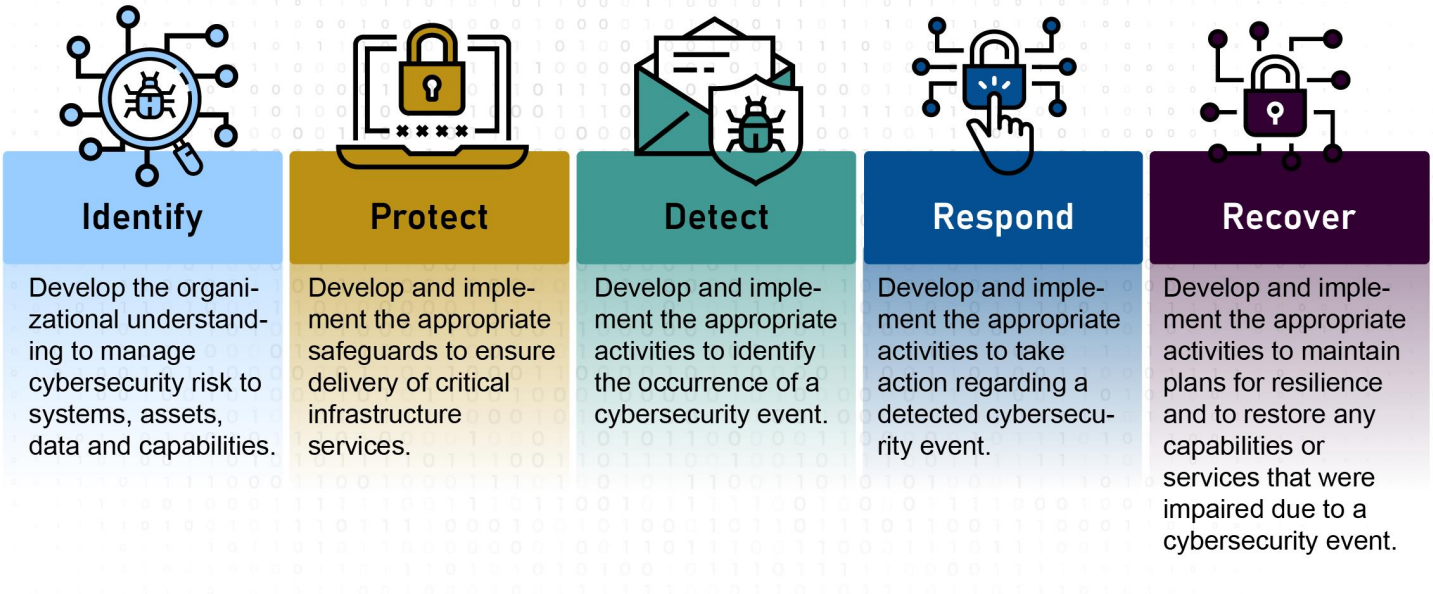
[15]Office of Management and Budget issued the latest report, the fiscal year 2022 report, on May 1, 2023. See Office of Management and Budget, *Federal Information Security Modernization Act of 2014, Annual Report Fiscal Year 2022* (Washington, D.C.: May 1, 2023).

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

[17]The Council of the Inspectors General on Integrity and Efficiency is an independent entity established within the executive branch to address integrity, economy, and effectiveness issues across government agencies.

cybersecurity risks.[18] In addition, agencies and their IGs use the framework in reporting on the maturity of agency information security policies and practices and the implementation of FISMA. The metrics used for FISMA reporting correspond to the core functions outlined in the framework. The NIST Cybersecurity Framework is based on five core security functions—identify, protect, detect, respond, and recover (see figure 3).

Figure 3: National Institute of Standards and Technology Cybersecurity Framework



Sources: GAO (analysis); lovemask/stock.adobe.com (icons); starlineart/stock.adobe.com (background). | GAO-24-106291

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.

[18]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).

OMB and CISA Established CIO Metrics

OMB and CISA collaborate with interagency partners to develop the CIO FISMA metrics. According to OMB, the metrics provide the data needed to monitor agencies' progress towards the implementation of the administration's priorities and best practices that strengthen federal cybersecurity. The metrics are established on an annual basis and include hundreds of data requests related to an agency's information security program. Agencies are to provide this information to OMB on a quarterly basis. According to OMB, the most recent CIO metrics for fiscal year 2023:

- align with executive order requirements to move toward zero trust architectures,[19]
- allow for automating certain reporting to ensure agencies can focus on outcomes over manual reporting, and
- establish a CISO Council FISMA Metrics Subcommittee that works to identify future metrics for automation in fiscal year 2024 and beyond.

OMB, DHS, and CIGIE Established Core IG Metrics

In addition to CIO metrics, OMB also collaborates with DHS and CIGIE to develop IG FISMA metrics. According to OMB, these metrics are intended to provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs. In fiscal year 2022, OMB implemented a new framework for the IG evaluations. The new framework, developed in collaboration with DHS and CIGIE, identified a set of core metrics that are to be assessed annually.

According to OMB, the core metrics represent a combination of Administration priorities, high impact risk reduction activities, and essential functions necessary to determine security program effectiveness. The framework also identified supplemental metrics that are to be assessed at least once every two years. OMB notes that these metrics represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. IGs were instructed to focus only on the core metrics for fiscal year 2022. OMB, DHS, and CIGIE continue to refine and update

[19]Zero trust architecture focuses on authenticating and authorizing every interaction between network resources and a user or device.

metrics annually to evaluate cybersecurity measures and align with federal priorities.

Executive Order Calls for Improvements in Cybersecurity

Executive Order 14028, issued in May 2021, stated that the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to cyber threats to the public and private sectors and the American people's security and privacy.[20] The order outlined actions that the Federal Government must take in five areas.

Modernize Federal Government Cybersecurity

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the federal government must take decisive steps to modernize its approach to cybersecurity. This includes increasing the federal government's visibility into threats, while protecting privacy and civil liberties. Among other things, the order stated that the federal government must advance toward zero trust architecture, which is a cybersecurity approach intended to address the rapidly evolving security risks faced by IT. The zero trust architecture approach focuses on authenticating and authorizing every interaction between network resources and a user or device.[21] The executive order also called for agencies to adopt multi-factor authentication and encryption for data at rest and in transit to the maximum extent consistent with federal records laws and other applicable laws.

Enhance Software Supply Chain Security

The security of software used by the federal government is vital to its ability to perform critical functions. Accordingly, the order states that the federal government must act to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software. This type of software performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources).

[20]The White House, Executive Order 14028, *Improving the Nation's Cybersecurity* (Washington, D.C.: May 12, 2021).

[21]For more information on zero trust architecture, see GAO, *Science & Tech Spotlight: Zero Trust Architecture*, GAO-23-106065 (Washington, D.C.: November 2022).

Standardize the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

The federal government must standardize its procedures for responding to cybersecurity vulnerabilities and incidents. According to the Executive Order, the procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting federal systems vary across agencies, hindering the ability to analyze vulnerabilities and incidents more comprehensively across agencies. In response to the Executive Order, CISA issued playbooks related to cybersecurity incident and vulnerability response in November 2021.[22]

Improve Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

Among other things, federal agencies are to enhance their capabilities to detect cybersecurity vulnerabilities and incidents by deploying endpoint detection and response capabilities to support proactive detection of cybersecurity incidents. Agencies are to also share data with CISA that are relevant to a threat and vulnerability analysis, as well as for assessment and threat-hunting purposes.

Improve the Federal Government's Investigative and Remediation Capabilities

The administration also called for improving the federal government's remediation and investigation capabilities through maintaining network and system logs. These logs are a valuable tool for addressing a cybersecurity incident on federal information systems. According to the Executive Order, the logs are to be protected by cryptographic methods to ensure integrity once collected.

Cybersecurity Strategy and Implementation Plan Outlines Administration's Approach to Better Secure Cyberspace

In March 2023, the White House released a National Cybersecurity Strategy and subsequently, in July 2023, released the accompanying

[22]Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident & Vulnerability Response Playbooks* (Washington, D.C.: November 2021).

implementation plan.[23] The strategy established five pillars to improve federal cybersecurity posture and enhance collaboration.

- **Defend Critical Infrastructure** by (1) establishing cybersecurity requirements to support national security and public safety, (2) scaling public-private collaboration, (3) integrating federal cybersecurity centers, (4) updating federal incident response plans and processes, and (5) modernizing federal defenses.
- **Disrupt and Dismantle Threat Actors** by (1) integrating federal disruption activities for malicious cyber activity, (2) enhancing public-private operational collaboration to disrupt adversaries, (3) increasing the speed and scale of intelligence sharing and victim notification, (4) preventing abuse of United States-based infrastructure, and (5) countering cybercrime and defeating ransomware.
- **Shape Market Forces to Drive Security and Resilience** by (1) holding the stewards of data accountable, (2) driving the development of secure Internet of Things devices, (3) shifting liability for insecure software products and services, (4) using federal grants and other incentives to build in security, (5) leveraging federal procurement to improve accountability, and (6) exploring a federal cyber insurance backstop.[24]
- **Invest in a Resilient Future** by (1) securing the technical foundation of the Internet, (2) reinvigorating federal research and development for cybersecurity, (3) preparing for our post-quantum future; (4) securing our clean energy future, (5) supporting development of a digital identity ecosystem, and (6) developing a national strategy to strengthen our cyber workforce.[25]
- **Forge International Partnerships to Pursue Shared Goals** by (1) building coalitions to counter threats to our digital ecosystem, (2) strengthening international partner capacity, (3) expanding the United States' ability to assist allies and partners, (4) building coalitions to reinforce global norms of responsible state behavior, and

[23]The White House, *National Cybersecurity Strategy* (Washington, D.C.: March 2023) and *National Cybersecurity Implementation Plan* (Washington, D.C.: July 2023).

[24]"Internet of Things" technology refers to devices collecting information, communicating it to a network and, in some cases, completing a task—like unlocking doors using a smartphone application. For more information, see GAO, *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Sept. 14, 2020).

[25]For information on post-quantum computing, see GAO, *Science & Tech Spotlight: Securing Data for a Post-quantum World*, GAO-23-106559 (Washington, D.C.: Mar. 8, 2023).

(5) securing global supply chains for information, communications, and operational technology products and services.

CIOs and IGs Reported Varied Progress in Implementing FISMA

As previously discussed, agencies are required to report the status of their information security programs to OMB through the CIO FISMA metrics. Agency IGs are to conduct annual independent assessments of those programs utilizing the IG FISMA metrics.

The status of the 23 civilian agencies' programs as reported through the CIO metrics varied. Although some improvement was reported from 2021 to 2022, IGs of 15 of the 23 civilian agencies found the information security programs to be ineffective. IGs reported various causes for ineffective information security programs, including management accountability issues and gaps in standards and quality control.

Agency Status in Implementing the Administration's Efforts to Strengthen Information Security Varied

The CIO FISMA metrics are intended to allow agencies and oversight bodies, such as OMB and DHS, to assess agencies' progress toward achieving outcomes and targets that strengthen federal information security, such as those related to administration priorities. According to the OMB-issued 2022 CIO metrics, the metrics were updated to include some of the requirements in Executive Order 14028. Although not always explicitly linked, we identified a subset of the 2022 CIO metrics that relate to the efforts the administration calls for in the order.

In aggregate, the 23 civilian CFO Act agencies varied in their status related to this subset of metrics. Table 1 below summarizes a subset of the CIO FISMA metrics related to administration priorities and the agency-reported status, in aggregate, for each.

Table 1: Civilian Chief Financial Officers Act of 1990 (CFO Act) Agencies' Status of Fiscal Year 2022 Federal Information Security Modernization Act (FISMA) Chief Information Officer (CIO) Metrics Relevant to Administration Priorities

Office of Management and Budget metric category	CIO metric	Agency-reported status of metric in fiscal year 2022
Enumerating the environment	Total of organization- and contractor-operated systems with an authority to operate (ATO)[a]	Of the total 6,218 federal information systems, 5,959 (95 percent) received an ATO, leaving 259 systems in operation without an ATO. Eleven agencies authorized 100 percent of their systems. One agency authorized only 54 percent of its systems.
Multifactor authentication (MFA)[b]	Number of systems that use MFA	Eighty-five percent of agencies' systems use MFA. Five agencies have a form of MFA for 100 percent of their systems.
Encryption	Number of systems that implement encryption for data at rest	For data at rest, federal agencies implemented encryption for 79 percent of their systems. Four agencies reported encrypting data at rest for all their systems.
	Number of systems that implement encryption for data in transit	For data in transit, federal agencies implemented encryption for 77 percent of their systems. Three agencies reported encrypting data in transit for all their systems.
Critical software security event logging[c]	Security events recorded for critical software	Federal agencies configured security event logging for 86 percent of their critical software. Fourteen federal agencies reported 100 percent implementation of security event logging for their critical software. Two agencies reported having no logs for security events for critical software.
Ground truth testing[d]	Number of systems that received ground truth testing	Twenty percent of federal agencies' information security systems received ground truth testing through automated means.
	Number of agencies with a red team[e]	Thirteen of the 23 civilian CFO Act agencies have a red team. Of all the 6,218 information systems at these agencies, 318 (5 percent) received a red team exercise.
Smart patching	Agencies with a centralized and/or automated patch management process	Sixty percent of federal agencies have a centralized patch management system. Seventy-three percent of agencies' patching processes leverage significant automation. Of the agencies that do have significant automation, an average of 79 percent of their software assets are covered by automation.
Resilience	Mean time to cybersecurity incident resolution	The mean time for federal agencies to resolve cybersecurity incidents was 20 days. While most agencies needed less than 20 days, two agencies required significantly more time—131 and 168 days—to resolve incidents.
	Number of systems that have a tested incident response plan	Federal agencies tested incident response plans for 76 percent of their information systems. Three agencies tested plans for 100 percent of their systems. However, one agency tested only 16 percent of its system incident response plans.

Source: GAO (analysis). | GAO-24-106291

Note: The Department of Defense was not included in our analysis of agencies because the department has classified the information in its FISMA report.

[a]An ATO is the official management decision given by a senior federal official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

[b]MFA is a mechanism used to verify an individual's identity by using more than just a username and password. It requires two or more of: something the user knows (password), something the user has (token), or something the user is (biometric).

[c]Critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; is designed to control access to data or operational technology; performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.

[d]Ground truth testing is a method to validate security control implementation and find weaknesses.

[e]A red team is authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an agency's security posture.

IGs Reported That Most Agencies Have Ineffective Information Security Programs in Fiscal Years 2021 and 2022

FISMA requires IGs to assess and report on the effectiveness of their agencies' information security programs using a capability maturity model developed by OMB, DHS, and CIGIE. As shown in table 2 below, 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.

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.
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 and mission needs.

Source: GAO analysis of Fiscal Years 2021 and 2022 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. | GAO-24-106291

Using the five-level maturity model described above, the IGs are to assign a maturity level rating for each of the five NIST Cybersecurity Framework

core functions—identify, protect, detect, respond, and recover.[26] After determining the maturity levels of the core functions, the IGs rate their agencies' overall information security programs as either effective or not effective.

According to OMB, a rating of level 4 (managed and measurable) or level 5 (optimized) is considered an effective level of security. However, IGs have the discretion, according to the FISMA evaluation guidance, to consider the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs. IGs are also encouraged to leverage supplemental reports (including past evaluations where results have had little variance year over year), and any additional evidence of information security program effectiveness to provide context within the evaluation period. For example, an IG may determine, given the particular circumstances of the agency, that a rating of level 3 (consistently implemented), rather than levels 4 or 5, will be considered effective.

In March 2022, we reported that the flexibility and discretion provided to the IGs in determining information security program effectiveness led to inconsistency in the way they were rating their agencies' programs.[27] This inconsistency resulted in ratings that were not easily comparable across the government. We recommended that the Director of OMB collaborate with its partners in DHS and CIGIE to create a more precise overall effectiveness rating scale for IG FISMA reports. OMB did not concur with this recommendation, and as of October 2023, had not implemented it.

According to a letter sent to us on December 5, 2023, from the OMB Director, the office does not agree that the existing rating scale lacks necessary precision. According to the Director, the effectiveness rating scale provides a strong toolset for determining the effectiveness and maturity of agency information systems and programs. The scale, according to the Director, also allows for significant context on levels of effectiveness and can be utilized in a manner that provides more nuanced information on the effectiveness of agency security programs and

[26]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (Gaithersburg, M.D.: Apr. 16, 2018).

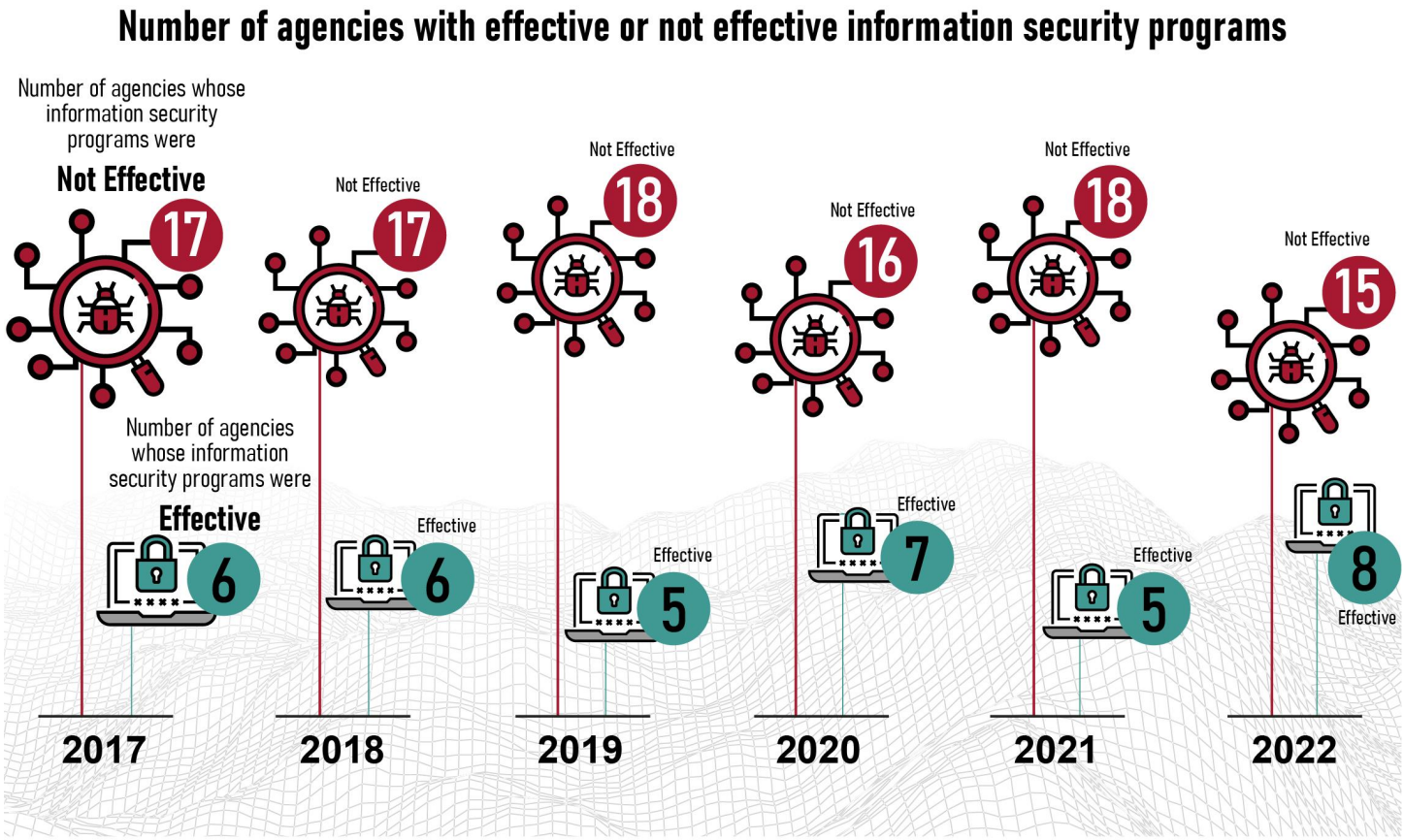
[27]GAO, *Cybersecurity: OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision*, GAO-22-104364 (Washington, D.C.: Mar. 31, 2022).

practices. Therefore, according to the Director, OMB does not plan to create a new or different FISMA rating scale.

However, as we stated in the March 2022 report, we maintain that implementing our recommendation would provide greater clarity to the ratings by more accurately reflecting agencies' implementation of security programs to both Congress and other oversight bodies. Further, our recommendation did 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.

Out of the 23 civilian CFO Act agencies, no more than eight received an effective rating in any given year over the last six years of reporting (fiscal years 2017 through 2022). In 2021, five agencies were considered to have an effective information security program—Environmental Protection Agency, General Services Administration, National Science Foundation, Nuclear Regulatory Commission, and the U.S. Agency for International Development. In the most recent reporting year, fiscal year 2022, three additional agencies received an effective rating from their IG—the Departments of Homeland Security, Education, and Justice. Conversely, the IGs reported that the remaining 15 agencies had ineffective information security programs. Figure 4 shows the number of the 23 civilian CFO Act agencies that IGs rated as effective or not effective in fiscal years 2017 through 2022.

Figure 4: Number of Civilian Agencies Subject to the Chief Financial Officers Act of 1990 That Do or Do Not Have Effective Information Security Programs, as Reported by Inspectors General, Fiscal Years 2017 through 2022



Sources: GAO (analysis); civilian agencies subject to Chief Financial Officers Act of 1990 (data); PST Vector/stock.adobe.com (background); lovemask/stock.adobe.com (icons). | GAO-24-106291

Note: We analyzed data reported by inspectors general for the 23 civilian agencies subject to the Chief Financial Officers Act of 1990, in response to the Federal Information Security Modernization Act (FISMA). We did not include the Department of Defense in our analysis of agencies because the department has classified the information in its FISMA report.

In addition to overall effectiveness, most agencies received a maturity score below level 4 for the five core functions outlined in the NIST Cybersecurity Framework. The highest rated core function for both fiscal years 2021 and 2022 was “respond.” The lowest rated core function was “recover” in 2021 with only two agencies receiving a maturity rating of level 4 or 5 for that function. In 2022, the lowest rated core function was “detect.” This indicates that most agencies are at a higher risk of not detecting a cyber security incident. Tables 3 and 4 show the IG’s individual functional area and overall effectiveness ratings for each of the 23 civilian agencies in fiscal years 2021 and 2022, respectively.

Table 3: Inspector General (IG) Maturity Level and Overall Ratings of the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Programs for Fiscal Year 2021

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

Legend: 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).

Sources: Office of Management and Budget and Inspectors General for civilian agencies subject to Chief Financial Officers Act of 1990 (data). | GAO-24-106291

Note: We did not include the Department of Defense in our analysis of agencies because the department has classified the information in its FISMA report.

[a]According to the Fiscal Year 2021 Core IG FISMA Metrics Evaluation Guide, maturity levels 4 and 5 are considered effective. The guide also noted that IGs should consider their own assessment of the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs. Therefore, ratings lower than level 4 could be considered effective by an agency's IG.

Table 4: Inspector General (IG) Maturity Level and Overall Ratings of the 23 Civilian Chief Financial Officers Act of 1990 Agencies' Information Security Programs for Fiscal Year 2022

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

Legend: 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).

Sources: Office of Management and Budget and Inspectors General for civilian agencies subject to Chief Financial Officers Act of 1990 (data). | GAO-24-106291

Note: We did not include the Department of Defense in our analysis of agencies because the department has classified the information in its FISMA report.

[a]According to the Fiscal Year 2022 Core IG FISMA Metrics Evaluation Guide, a Level 4—managed and measurable—information security program is still considered to be operating at an effective level of security. The guide also noted that IGs should consider their own assessment of the unique missions, resources, and challenges faced by their agency when assessing the maturity of information security programs. Therefore, ratings lower than level 4 could be considered effective by an agency's IG.

IGs Identified Lack of Management Accountability and Other Causes of Ineffective Information Security Programs

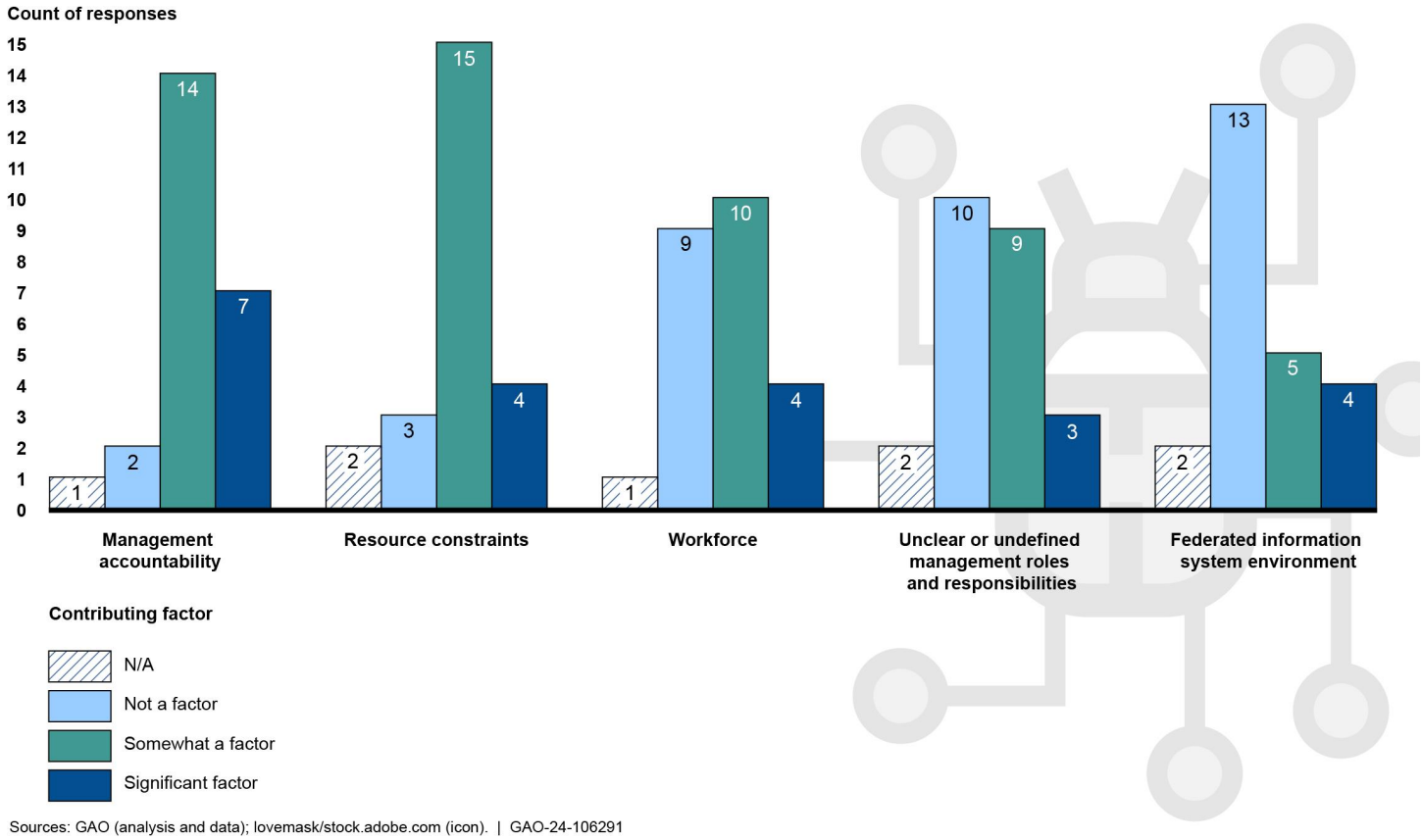
IGs reported various causes for weaknesses in agencies' information security programs that contribute to agencies' ineffective ratings. Specifically, IGs from all 24 CFO Act agencies, including the Department of Defense, shared their perspectives on the extent to which the following reasons contributed to ineffective information security programs at their agency.

- **Management accountability issues** were reported by 21 of the 24 IGs. For example, one IG stated that there is a lack of accountability to perform information security-related roles and responsibilities, as well as a lack of oversight to ensure consistent implementation. Other IGs cited high turnover rates at the leadership level as another example.
- **Resource constraints** were reported by 19 IGs. The most common issue cited was an inadequate IT budget. IGs reported that agency budgets are not always large enough to procure all the needed software and tools to meet policy requirements.
- **Workforce challenges** were reported by 14 IGs. IGs reported that agencies had challenges in recruiting and retaining a qualified cyber workforce with the right knowledge and capabilities. IGs also cited significant turnover rates as a cause for ineffective information security programs.
- **Unclear or undefined management roles and responsibilities** were reported by 12 IGs. For example, one IG stated that an agency cannot implement or enforce IT policies or procedures if the roles and responsibilities of those tasked to do so are not clearly defined and communicated.
- **Federated information system environment challenges** were reported by nine IGs.[28] For example, IGs reported that agencies had challenges due to the inability to fully assess all systems, specifically at the component level. IGs stated that components do not always share information about their systems with the department-level agency.

[28]A federated agency is one where divisions, or components, within the agency are responsible for governance within their respective organizations.

Figure 5 shows the extent to which IGs said each of the causes identified above contributed to ineffective information security programs.

Figure 5: Perspectives from the 24 Chief Financial Officers Act of 1990 Agency Inspectors General on the Causes of Ineffective Information Security Programs



Sources: GAO (analysis and data); lovemask/stock.adobe.com (icon). | GAO-24-106291

Accessible Data Table for Figure 5: Perspectives from the 24 Chief Financial Officers Act of 1990 Agency Inspectors General on the Causes of Ineffective Information Security Programs

	N/A	Not a factor	Somewhat a factor	Significant factor
Management accountability	1	2	14	7
Resource constraints	2	3	15	4
Workforce	1	9	10	4
Unclear or undefined management roles and responsibilities	2	10	9	3
Federated information system environment	2	13	5	4

Source: GAO (analysis and data): lovemask/stock.adobe.com (Icon) | GAO-24-106291

Note: We analyzed questionnaire responses by inspectors general for the 24 agencies subject to the Chief Financial Officers Act of 1990 on the causes of ineffective information security programs.

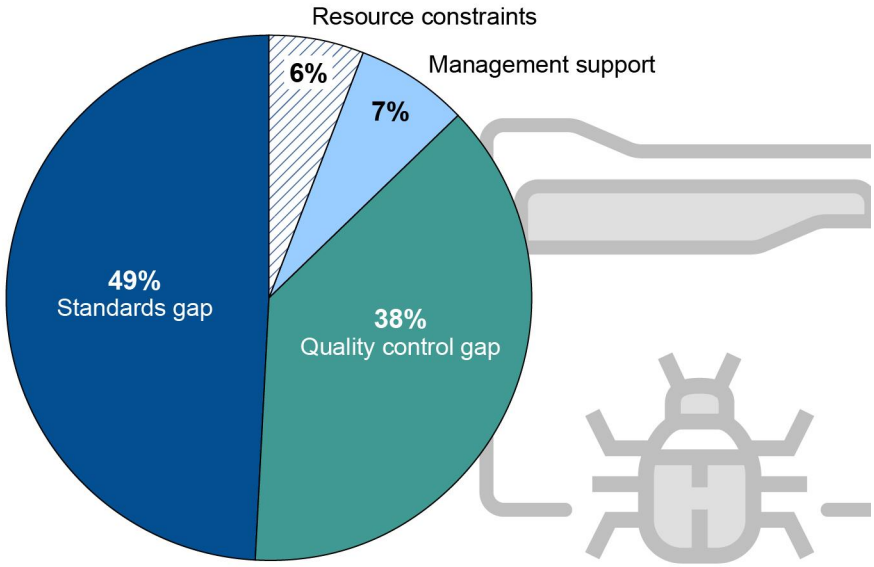
In addition, four general causes for agencies' information security program weaknesses were identified in IG FISMA audit reports for fiscal year 2022.[29]

- **Gaps in standards:** Agency policies, procedures, or standards were unclear; outdated; or not yet developed.
- **Gaps in quality control:** Agency had not fully implemented processes to ensure requirements were met.
- **Management support:** Agency management made the decision not to take actions that would have addressed a weakness.
- **Resource constraints:** Agency lacks the personnel or funding to address a weakness.

The most common reported causes of weaknesses in agency information security programs were gaps in standards and quality control. Figure 6 summarizes the frequency of reported causes of program ineffectiveness. Addressing these various causes of information security program weaknesses through appropriate FISMA metrics could help to improve the cybersecurity posture across federal agencies.

[29]We did not include Department of Defense in the review of general causes because the department classified the inspector general's FISMA metrics report.

Figure 6: Causes of Program Ineffectiveness for the 23 civilian Chief Financial Officers Act of 1990 Agencies Reported by Inspectors General in Fiscal Year 2022



Sources: GAO (analysis); Inspectors General for civilian agencies subject to Chief Financial Officers Act of 1990 (data); Gofficon/stock.adobe.com (icon). | GAO-24-106291

Note: We analyzed data reported by inspectors general for the 23 civilian agencies subject to the Chief Financial Officers Act of 1990, in response to the Federal Information Security Modernization Act (FISMA). We did not include the Department of Defense in our analysis of agencies' performance data because the department has classified the information in its FISMA report. Percentages are based on the frequency a cause was identified for information security program deficiencies reported in the Inspectors General for fiscal year 2022 Federal Information Security Modernization Act audit reports.

A Variety of Practices Contributed to Improvement in Information Security Programs' Effectiveness

Agencies have taken actions to implement FISMA requirements intended to improve their information security posture. Due to differences in agency size, resources, and mission, agencies have taken varied approaches to strengthening their information security programs. Selected agencies identified practices that resulted in positive outcomes for their information

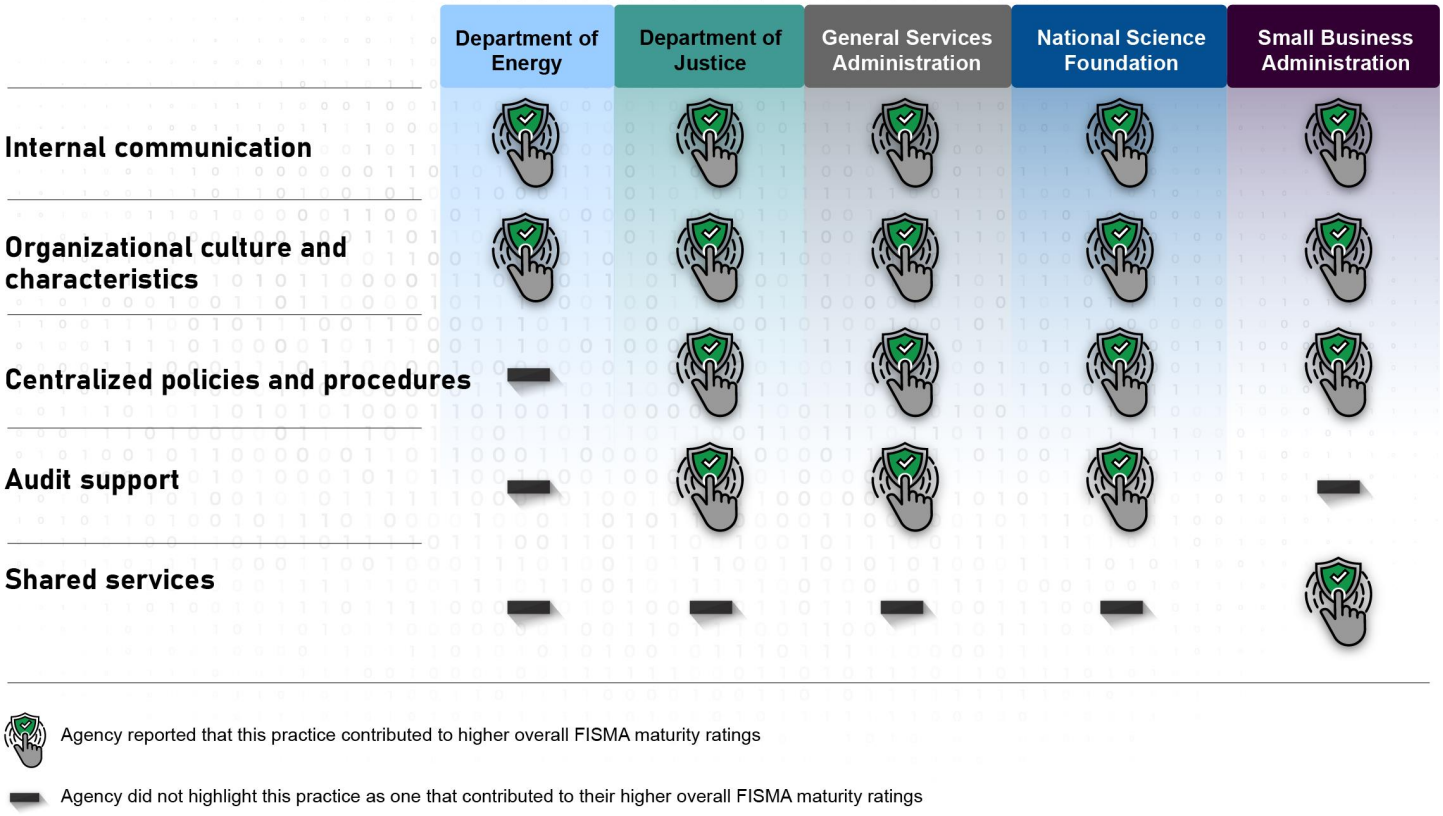
security programs and implementation of FISMA.[30] In particular, agency officials most commonly reported that internal communication, as well as organizational culture and characteristics contributed positively to FISMA implementation efforts.[31]

For a full list of the practices highlighted by agency officials, see appendix II. Figure 7 shows the practices highlighted the most by these agencies.

[30]The five selected agencies are the Departments of Energy and Justice, General Services Administration, National Science Foundation, and Small Business Administration. Agency officials discussed a variety of information security practices that we categorized based on common themes.

[31]Agency officials included individuals from the Office of the Chief Information Officer, Office of the Chief Information Security Officer, Office of the Inspector General, and relevant information security contractors, among other officials.

Figure 7: Practices Highlighted by Selected Agencies as Contributing to Higher Overall Federal Information Security Modernization Act of 2014 (FISMA) Maturity Ratings



Sources: GAO (analysis and data); selected civilian agencies subject to Chief Financial Officers Act of 1990 (data); lovemask/stock.adobe.com (icons); starlineart/stock.adobe.com (background). | GAO-24-106291

Note: We analyzed documentation and interviews from selected agencies subject to the Chief Financial Officers Act of 1990.

Internal Communication

Officials from all five selected agencies highlighted internal communication as a practice that resulted in positive outcomes for their information security programs and implementation of FISMA. For example, officials stated that they have implemented agency-wide information security groups and hold individual meetings with information security program officials.

According to officials from two of the five selected agencies, these practices mitigated challenges associated with their federated

environments. Additionally, officials from all selected agencies, stated that coordination among these groups improved the consistency of FISMA implementation.

For example, the Department of Energy established several groups to coordinate across the organization more effectively. To illustrate, the department established a quarterly CIO and CISO summit and an executive council to enable broader communication and collaboration on departmental information security strategy. Officials stated that such communication has benefited their information security posture. The department has also organized communities of practice and working groups to coordinate its information security efforts.

According to agency officials, the Department of Justice's Office of the Chief Information Officer (OCIO) holds weekly status meetings with components to discuss information security weakness remediation efforts and compliance with department-wide requirements. These meetings, according to department officials, also provide a space for teams to effectively coordinate. The department also implemented a dashboard in support of its enterprise continuous monitoring program. Officials stated that this dashboard is integrated with departmental information security tools, and provides detailed data on asset management, configuration management, and vulnerability management. Department of Justice officials noted that the dashboard provides real-time data from components that enables the OCIO to better monitor and manage them.

According to the agency, the National Science Foundation's Division of Information Systems meets daily to discuss its information security program, incidents and incident response, and infrastructure changes. Additionally, agency officials that lead FISMA-related efforts periodically meet with the CISO and CIO to discuss the agency's information security posture and provide an overview of quarterly FISMA metrics.

Organizational Culture and Characteristics

Officials at each of the selected agencies stated that characteristics unique to their organization better positioned their agency to meet FISMA requirements. This included commitment of agency leadership, as well as organizational structure and size. These unique characteristics, according to these agencies, allowed them to facilitate better coordination, maintain awareness of information security, and more easily implement new technology.

Department of Justice officials stated that its leadership is committed to improvement and is good at finding resources to address information security needs. Additionally, officials added that the department's leadership is well-informed of its information security status and IG audit findings. According to officials, the department's leadership emphasizes closing recommendations quickly.

Officials at the General Services Administration also cited leadership commitment as key to helping them meet FISMA requirements. Specifically, officials stated that agency leadership places importance in achieving optimized ratings (or level 5) on the FISMA evaluation.

Likewise, National Science Foundation officials stated that agency leadership takes FISMA implementation seriously and that their commitment encouraged staff to be equally as dedicated to improving the agency's information security program. Officials stated that staff can candidly discuss IG recommendations with agency leadership and that there was an organizational culture to strive for high FISMA ratings.

Additionally, officials from two agencies—General Services Administration and National Science Foundation—stated that the centralized nature of their organization allowed for more consistent implementation of FISMA requirements. General Services Administration officials stated that having fewer components allowed them to implement new information security tools in a more efficient way. These officials also stated that the agency has implemented an Ongoing Authorization Program, which provides a centralized oversight mechanism for information security assessments.[32]

Officials at the National Science Foundation also commented about the agency size being a benefit. Specifically, officials stated that the smaller size of the agency allowed them to easily communicate updates to policies and procedures, as well as provide oversight for and coordination of information security implementation. They stated that, compared to other agencies, they are smaller, less complex, and had fewer internal organizations to work with; making it easier to implement information security requirements and fix issues.

[32]General Services Administration established the Ongoing Authorization Program to enable FISMA systems to maintain their authorization to operate on a continuous basis. Systems within this program are assessed at a higher frequency and are expected to meet a high level of compliance across various IT management and cyber hygiene requirements.

Centralized Policies and Procedures

Most of the selected agencies highlighted the centralization of their policies and procedures as a contributor to improving their effectiveness in information security. Officials stated that having centralized processes helped align components with FISMA requirements and improved the agencies' information security posture.

For example, at the Department of Justice, components may develop their own policies and guidance provided they meet department-level minimum information security policy requirements. Agency officials stated that alignment with centralized information security policies and guidance has improved the information security posture of departmental components. The department has centralized information security policy and guidance resources related to vulnerability management, continuous monitoring, and configuration management, among others.

As another example, the Small Business Administration's Office of the CIO established an Information Security Division that is responsible for designing, implementing, and maturing security practices to protect critical business processes and IT assets across the organization. For example, the division has defined certain minimum requirements for the onboarding and readiness of new systems as a part of the agency's efforts to centralize the management of its systems. New systems must follow guidance that includes requirements for system inventory, vulnerability scanning, system security plans, enterprise security monitoring, penetration testing, privacy requirements, and multi-factor authentication. The division has also defined baseline logging requirements to ensure proper monitoring of systems.

Audit Support Activities

Three agencies—the Department of Justice, General Services Administration and National Science Foundation—conducted activities to support and improve audit responsiveness to IG requests and recommendations. This included activities such as coordination with the IG, audit preparedness, and review of audit results. Agency officials stated that such activities helped improve their information security posture.

For example, the General Services Administration officials stated that they have an effective working relationship with the IG and have a proactive approach to the FISMA evaluation. Officials explained that they

routinely exchange information about the evaluation through a series of formal and informal meetings throughout the year. To illustrate, the OCIO holds audit status meetings with the IG to review accomplishments, remaining work, and lessons learned. Additionally, the OCIO meets with the IG at least twice a year to review planned audits and share prior or anticipated challenges.

As part of the agency's audit support, the General Services Administration coordinates with relevant officials to prepare pre-audit checklists to monitor the information security status of its systems. Agency officials stated that these checklists are based on systemic challenges, recurring findings, and deliverables in alignment with the FISMA metrics. Additionally, the agency conducts self-assessments of each of the NIST cybersecurity framework functional areas. In conducting the self-assessment, the agency provides the IG justifications and supporting documentation for their self-identified ratings. General Services Administration officials stated that these types of activities help to demonstrate progress to the IG.

Shared Services

The Small Business Administration highlighted shared services as a way to improve consistency between components. For example, officials stated that they are transitioning toward centralizing their information security tools. The agency encourages the use of existing tools—such as those for endpoint protection, network monitoring and management, data security and privacy, vulnerability management, patch management, and continuous monitoring—to avoid acquiring new contracts. Additionally, the officials added that they perform occasional walkthroughs of these tools to provide an opportunity to identify gaps and needs.

Agencies Suggest That OMB Should Modify Metrics to Better Measure Information Security Effectiveness

As previously discussed, OMB works with several groups to develop performance metrics intended to evaluate the extent to which agencies have effectively implemented FISMA. These groups are the:

- **Cybersecurity and Infrastructure Security Agency**, an agency under DHS, that partners with OMB to develop and annually issue the CIO FISMA metrics and guidance.
- **Council of the Inspectors General on Integrity and Efficiency**, an independent entity established within the executive branch that partners with OMB, DHS, and other stakeholders to develop the IG FISMA metrics and assessment guidance.
- **Federal Chief Information Security Officer Council**, an interagency forum led by the Federal CISO that provides feedback to OMB on the FISMA metrics.

Agencies and IGs are to use the metrics that these groups develop to evaluate the effectiveness of information security programs. However, several agencies and their inspectors general stated that they did not always believe the FISMA metrics were a useful measure because, in some cases, they do not accurately evaluate whether an agency has an effective information security program. In general, 12 of 24 OCIOs and 10 of 23 IGs from the 24 CFO Act agencies believe that FISMA metrics do not always accurately evaluate the effectiveness of their information security program.[33]

The 24 CFO Act agencies and their IGs provided various perspectives on areas where they believe the FISMA metrics should be further modified to better measure the effectiveness of information security programs across the federal government. These areas relate to performance goals, workforce, agency size, and risk-based approaches.

Performance Goals

Twenty-one of the 24 OCIOs reported that FISMA CIO metrics should be clearly tied to performance goals. While the CIO metrics require agencies to report on hundreds of data points, some do not include targets, or goals that the agency should be striving to achieve. For example, 15 of 24 OCIOs reported that the metrics related to ground truth testing do not include specific targets.[34] One agency OCIO reported that these metrics are difficult to quantify as measures of effectiveness because they only

[33]According to the General Services Administration IG officials, they could not provide a response to the question regarding the effectiveness of the IG metrics because their contractor, not agency IG officials, conducts the FISMA audit.

[34]Ground truth testing consists of methods that empirically validates and verifies information security and finds weaknesses and can include, for example, penetration testing.

provide insight into what is or is not occurring. The OCIO officials said that there is no clear performance goal for what agencies should be striving for in order to be seen as good performers.

An Agency's View on How Cross Agency Priority (CAP) Goals Provided Measurable Targets

"OMB needs to immediately reinstate the cyber CAP Goal reporting, which stems from the President's Management Agenda (PMA). The PMA lays out a long-term vision and publicly tracks progress on achieving a series of targets and milestones. There were ten cyber CAP priority security capability areas for the federal agencies to meet. Without cyber CAP metrics, it is as though an important pillar of agency information security program effectiveness is missing."

Source: Agency's Responses to GAO Questionnaire. | GAO-23-106291

One agency's OCIO officials noted that the metrics are only partly useful when they are not clearly tied to targets and goals. The officials added that the usefulness of any metric depends on how the data is used to measure performance aligned with tangible actions and objectives. According to the OCIO officials, without information on how the metrics are used, programs can only assume what constitutes a good versus poor performance for the metrics. Another OCIO echoed this concern, stating that agencies are often left to interpret the intent of the metric, which can cause inaccurate reporting.

Other agencies cited the lack of Cross Agency Priority (CAP) goals as a challenge with accurately measuring information security program effectiveness. Historically, CAP goals were intended to measure federal progress toward implementing the President's Management Agenda. However, the current administration has not released specific cyber-related CAP goals since the issuance of the new agenda, the Biden-Harris Management Agenda Vision, in November 2021.

Workforce

Agency-Suggested Workforce Metrics

"What is your total necessary cybersecurity positions? How many of these positions are funded? How many of these positions are currently filled? What is your total necessary cybersecurity budget necessary to meet all current requirements? What is your current funding level?"

Source: Agency's Responses to GAO Questionnaire. | GAO-23-106291

Ten out of 24 OCIOs and 12 out of 24 IGs reported that the workforce metrics should be modified to better address workforce challenges. For example, OCIO officials and IGs at several agencies stated that metrics related to resources, recruitment and retainment, and cyber skills gaps should be added. Other agency OCIOs reported that they would like the FISMA metrics to incorporate questions on workforce roles that are more related to the IT industry, such as data analytics, program management, testing, and policy analysis.

Agency Size

Eleven of 24 OCIOs and 10 of 24 IGs reported that the FISMA metrics need to be modified to account for the size of the agency. These officials noted that when reporting the status of cybersecurity across the federal government, agencies should be compared based on their similarities in workforce size, operating budgets, ratio of sensitive data, and the total number of assets.

Several agency OCIO and IG officials stated that large, federated agencies have more distributed risk management approaches compared to smaller agencies. The officials added that smaller agencies tend to have more robust FISMA audits due to the lack of multiple operating divisions that larger agencies have. Conversely, according to the officials, larger agencies focus more on policies and procedures with limited testing at each operating division due to time constraints. Thus, the officials noted, the audit can become repetitive as some large components of the agency are selected for review each year and the IGs are asking them for the same documentation on an annual basis.

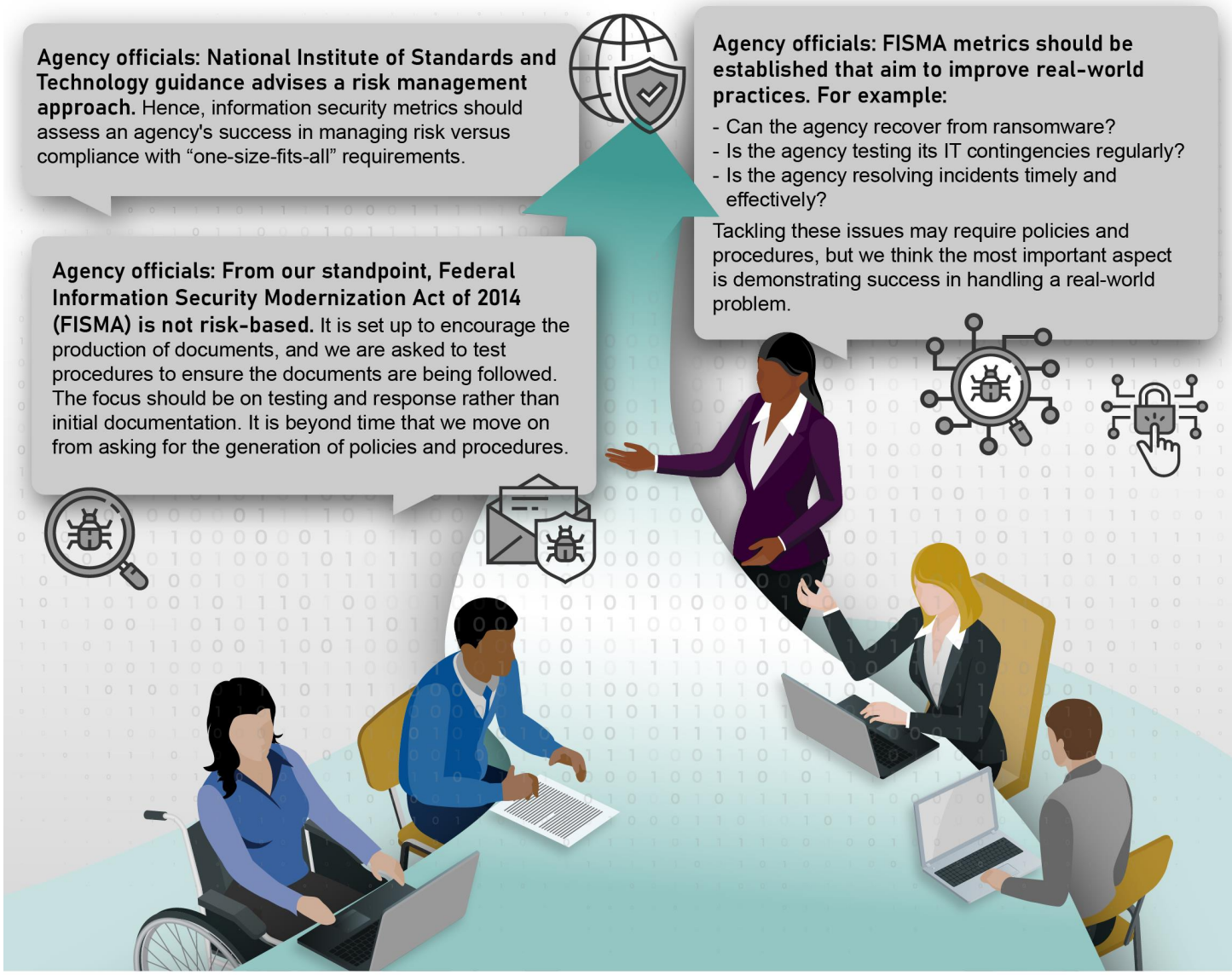
To that end, one IG's officials suggested that OMB should modify the metrics by creating a three-tiered system, in which there is a level for larger agencies, mid-size agencies, and smaller agencies. Another IG's officials suggested that the annual metrics should be divided into two sets of metrics in order to tailor them according to the size and scope of a federal agency. Thus, according to the IG officials, agencies that are similar in size, funding, scope, and organization could be tested and compared based on their system risk levels.

Risk-based Approach

Although FISMA and federal policies emphasize that agencies take a risk-based approach to cybersecurity by identifying, prioritizing, and managing their cyber risks, agencies often reported that the FISMA metrics focus on compliance and not risk. Specifically, 15 of 24 OCIOs and nine of 24 IGs reported that the FISMA metrics should be modified to focus more on risk instead of compliance.

Several agency IG officials agreed that FISMA audits should reflect the agencies' abilities to handle real-world cybersecurity issues, rather than their ability to create policies and procedures to achieve FISMA compliance. According to these officials, doing so would ensure more accurate FISMA reports and better measure the effectiveness of federal information security programs. Figure 8 shows examples of agencies' views on how FISMA metrics should be modified to account for risk.

Figure 8: Examples of Federal Agencies' Views on How FISMA Metrics Should Be Modified for Risk



Sources: GAO (analysis); Golden Sikorka/stock.adobe.com (people); starlineart/stock.adobe.com (background); lovemask/stock.adobe.com (icons). | GAO-24-106291

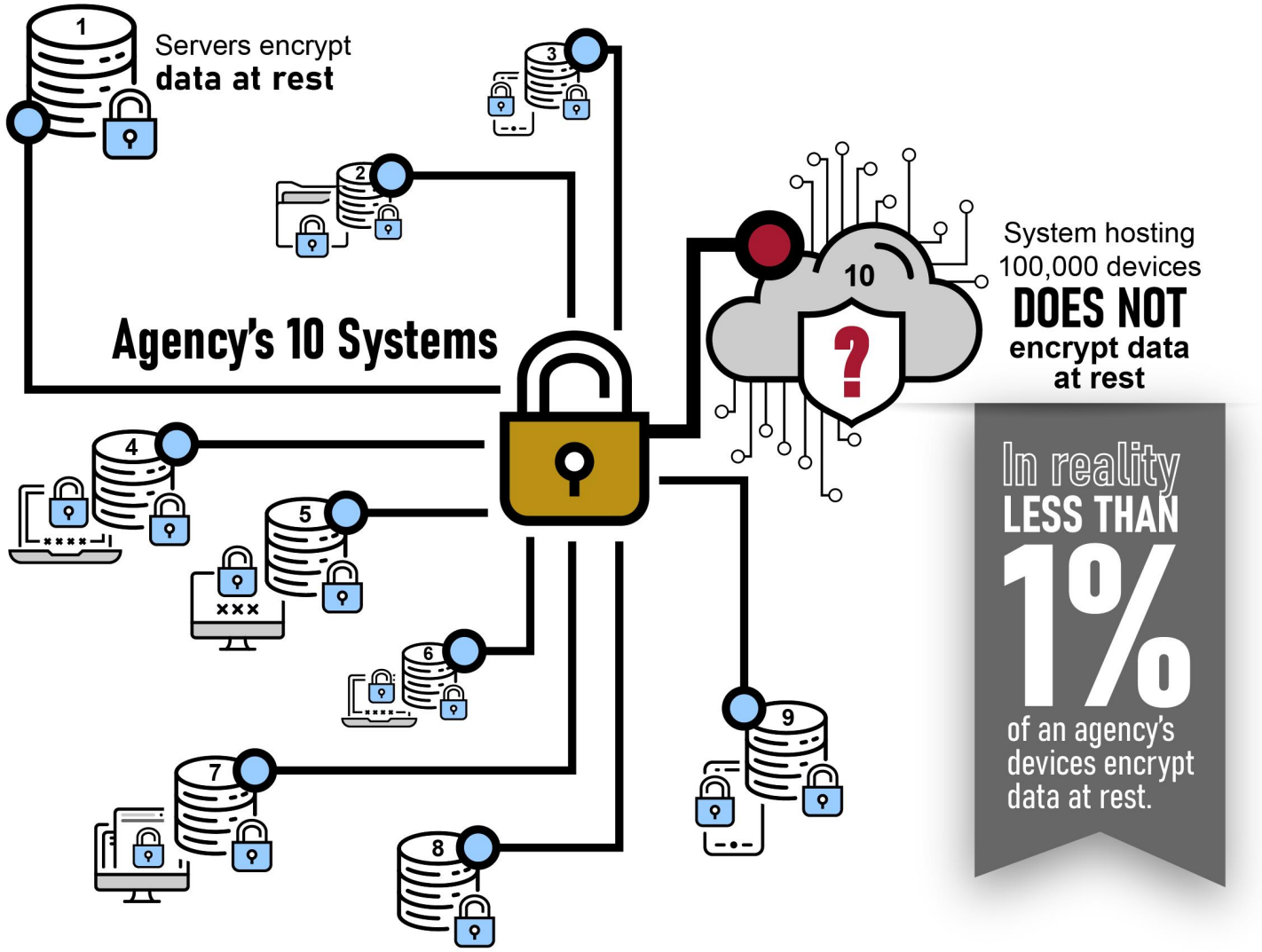
In addition to the areas for improvement discussed above, agencies also noted that the FISMA metrics do not always provide a clear picture of how well the federal government is doing in achieving its information security goals. For example, one agency's OCIO officials stated that metrics

seeking 100 percent compliance or implementation often lack context to identify unique or complex use cases that limit full adoption. The officials said agencies should be requested to provide additional information for these situations to contextualize why 100 percent compliance may not be realistically achievable, but that appropriate controls are in place to mitigate the risks.

Another agency's OCIO officials provided a real-world example of how FISMA metrics may not provide an accurate picture of an agency's data at rest encryption implementation—one of the CIO metrics agencies are asked to address.[35] As figure 9 depicts, an agency could have ten systems, nine of which consist of one server that encrypts data at rest. The tenth system, consisting of 100,000 devices that store sensitive data, does not encrypt data at rest. Because the agency is asked to provide the number of systems that encrypt data at rest, the agency's FISMA audit may show that 90 percent of its systems encrypt this data. However, the actual number of devices that are encrypting data at rest is less than one percent.

[35]Data at rest refers to data that is not being accessed and is stored on a physical or logical medium.

Figure 9: Example of How Federal Information Security Modernization Act of 2014 (FISMA) Metrics May Not Provide an Accurate Picture of An Agency's Encryption Implementation



Agency officials: FISMA metrics may not provide an accurate picture of an agency's data at rest encryption implementation. An agency could have 9 systems, comprised of one server each, that encrypt data at rest. The 10th system could consist of 100,000 devices that do not encrypt data at rest. In this case, FISMA metrics would show that 90% of the agency's systems encrypt data at rest.

Sources: GAO (analysis and data); Gofficon/stock.adobe.com (cloud icon); lovemask/stock.adobe.com (all other icons). | GAO-24-106291

Note: We analyzed responses to a questionnaire and data collection instrument from agencies subject to the Chief Financial Officers Act of 1990.

According to OMB, the metrics are meant to reflect reporting requirements that are needed to monitor agencies' progress towards the implementation of the administration's priorities. In commenting on a draft of this report, OMB officials stated that creating FISMA metrics based on size of agency or budget authority would create additional challenges, such as cross-government inconsistencies and lack of standardization, which would compromise comparability. However, as previously discussed, multiple agencies and IGs reported that given the complexity and differences in each agencies' information security programs, comparing one small agency to a large, highly complex agency may not be appropriate.

In December 2022, OMB established the CISO Council FISMA Metrics Subcommittee that is tasked with advising them on areas where FISMA guidance and metrics should be refined and improved. OMB officials stated that the subcommittee receives numerous suggestions from agencies, including the suggestions above, on how the metrics should be revised and must prioritize those revisions. The officials added that the metrics cannot all be substantially changed from year to year or progress may not be measured.

While this is a positive step, these agency perspectives indicate that FISMA metrics do not always provide a clear picture of how the federal government is achieving its goals related to information security. Until OMB has a consistent and accurate picture of agencies' information security performance, it will be challenged in determining where agencies are in achieving a strong cybersecurity posture.

Conclusions

Thousands of reported cybersecurity incidents each year underscore the importance of federal agencies implementing and maintaining effective information security programs. Although reported effectiveness has recently increased, the majority of reviewed federal agencies continue to be deemed ineffective. IGs identified various causes that contributed to the ineffective information security programs, including a lack of management accountability. Addressing these causes through appropriate metrics is critical to increasing the effectiveness of programs.

While selected agencies have implemented practices that have improved the effectiveness of their information security programs, numerous agency CIOs and IGs offered suggestions on how FISMA metrics could

be modified to more accurately measure progress in agencies meeting Administration priorities. Implementing these suggestions in the areas of performance goals, workforce challenges, agency size, and risk could help OMB and the FISMA Metrics Subcommittee ensure that future ratings present a more consistent and accurate overall picture of federal agency effectiveness and achievement of relevant goals and priorities.

Recommendations for Executive Action

We are making the following two recommendations to OMB:

The Director of OMB, along with its collaborative partners in DHS, should develop FISMA metrics related to causes of ineffective information security programs identified by IGs, such as management accountability and gaps in standards and quality control. (Recommendation 1)

The Director of OMB, along with its collaborative partners in DHS and CIGIE, should improve the CIO and IG FISMA metrics to clearly link them to performance goals, address workforce challenges, consider agency size, and adequately address risk. (Recommendation 2)

Agency Comments

We requested comments on a draft of this report from OMB and the 24 CFO Act agencies. In response, OMB, the one agency to which we made recommendations, neither agreed nor disagreed with them but provided technical comments, which we incorporated as appropriate. Of the 24 CFO Act Agencies, four generally agreed with our recommendations to OMB, and the remaining 20 did not provide substantive comments on the draft report. In addition, three of the 24 agencies provided technical comments, which we incorporated as appropriate.

The Departments of Agriculture, Defense, and Labor and the Nuclear Regulatory Commission stated via email from agency liaisons that they generally agreed with our recommendations to OMB and had no other comments on the draft report.

Twenty agencies did not provide substantive comments on the contents of the report. In particular, in its written comments, the Social Security Administration Chief of Staff stated that the agency appreciated the opportunity to review the draft but had no comments on it. The agency's

letter is reprinted in appendix III. The U.S. Agency for International Development's Assistant Administrator for the Bureau for Management stated in written comments that the agency is committed to supporting improvements to manage information system security and comply with federal cybersecurity policies and practices. The agency's comments are reprinted in appendix IV. Fifteen agencies informed us via email that they had no comments on the draft report. These agencies were the Departments of Commerce, Education, Energy, Homeland Security, Housing and Urban Development, State, Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Office of Personnel Management, and Small Business Administration. The Departments of Health and Human Services, Justice, and the Interior provided technical comments, which we incorporated as appropriate.

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

If you or your staff have any questions about this report, please contact Jennifer R. Franks 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 III.

Jennifer R. Franks, Director
Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The Federal Information Security Modernization Act of 2014 (FISMA) includes a provision for GAO to periodically evaluate federal agencies' information security policies and practices.[1] Our specific objectives for this assessment were to identify (1) the reported effectiveness in agencies' efforts to implement FISMA; (2) the key practices used by agencies to meet FISMA requirements; and (3) how FISMA metrics could be changed to better measure the effectiveness of federal agency information security programs.

To address the first objective, we analyzed information from the annual FISMA assessments issued by the 23 civilian Chief Financial Officers Act of 1990 (CFO Act) agencies' IGs for fiscal years 2021 and 2022.[2] We also analyzed information from the agencies' annual FISMA Chief Information Officer (CIO) reports for fiscal year 2022. We compared the information in the reports to Executive Order 14028, titled Improving the Nation's Cybersecurity, to identify a subset of the metrics that relate to the administration's efforts to improve cybersecurity. We then aggregated the information across all 23 civilian agencies and summarized the results of the selected subset of CIO metrics.

We then relied on the analysis to develop an overview of the state of federal cybersecurity and a summary of government-wide FISMA implementation. In addition, we reviewed the IGs' fiscal year 2021 and 2022 maturity level ratings for their agencies in each of the five core

[1]Pub. L. No. 113-283, § 3555, 128 Stat. 3073, 3083 (Dec. 18, 2014).

[2]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 report of agencies' performance data because the department has classified the information in its FISMA reports.

functions identified in the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.[3]

Further, we reviewed FISMA information security audit reports issued by IGs to determine whether they identified any causes for ineffective information security program deficiencies. Where identified, we then categorized the causes to determine the most commonly identified causes. To further this analysis, we developed a questionnaire to determine the extent to which certain common challenges, identified in our analysis of IG FISMA reports and during discussions with IG officials, were also causes for common findings of ineffective information security programs. We administered the questionnaire to all 24 CFO Act agencies, including the Department of Defense. We took steps to help ensure the reliability of the data collected. Specifically, we conducted a pretest of the questionnaire with GAO's Chief Information Security Officer to ensure that the questions were clear, unbiased, and consistently interpreted. The pretest allowed us to obtain initial feedback and helped ensure that officials understood the questions. We also conducted follow-up interviews with agency officials, where necessary, for clarification on their responses.

To address the second objective, we solicited agency perspectives on the practices they have implemented resulting in positive outcomes for their information security programs and implementation of FISMA. To gain these perspectives, we conducted semi-structured interviews with Office of the Chief Information Officer (OCIO), Office of the Chief Information Security Officer (OCISO), and Office of the Inspector General (IG) officials from selected civilian CFO Act agencies.

To select the sample of agencies, we developed a list of civilian CFO Act agencies and compiled the composite score of functional areas as reported in the Office of Management and Budget's (OMB) Fiscal Year 2021 FISMA Report.[4] For the purposes of this review, we considered agencies with a composite score of 15 or greater for the NIST

[3]OMB requires Inspectors General (IG) to assess the effectiveness of information security programs on a five-level maturity model. These levels are: (1) ad hoc, (2) defined, (3) consistently implemented, (4) managed and measurable, and (5) optimized. OMB considers maturity levels of four and five to be effective. However, IGs have the discretion to determine the rating of their agency's overall effectiveness or functional area at the maturity level of their choosing.

[4]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2021* (Washington, D.C.: Sep. 14, 2022).

Cybersecurity Framework five functional areas.[5] From this population, we selected a stratified random sample to get perspectives on the practices at agencies of different sizes and missions. Specifically, we categorized agencies as small, mid-size, and large based on their fiscal year 2021 internal funding as reported to the federal IT Dashboard.[6] We used a randomization formula within each size category to select two agencies from each category to interview, resulting in an initial selection of six agencies.

To obtain information on selected agency practices, we interviewed officials knowledgeable of the agency's information security program practices. Specifically, we asked participants to discuss their thoughts on

- the practices the agency has implemented that they felt led to effective FISMA implementation,
- how the agency measures the effectiveness of its actions, and
- other factors that may have positioned the agency to achieve FISMA-related goals.

In addition, we obtained documentary evidence of the various practices discussed by agency officials. Further, we met with officials from each agency's IG to validate information from agency officials and gain their perspective on the practices identified by the agency. In our efforts to validate the information from agency officials, one of the six selected agencies was removed from our original sample due to inconsistencies noted by their IG. Therefore, our review included five selected agencies—Departments of Energy and Justice, the General Services Administration, the National Science Foundation, and the Small Business Administration.

To address the third objective, we identified the organizations charged with developing and evaluating the effectiveness of FISMA metrics. We also identified and reviewed the CIO and IG FISMA metrics and guidance documentation. Further, we solicited the perspectives of each of the 24 CFO Act agency OCIOs and IGs on the FISMA metrics. In addition to the questionnaire described above for objective one, we used two data collection instruments and questionnaires to ask agencies and their IGs about their opinion on the usefulness of each FISMA metric. The OCIOs

[5]Each of the five functional areas can have a maximum score of five, for a total of 25.

[6]The federal IT Dashboard is a public, federal government website previously operated by OMB and currently by GSA at https://itdashboard.gov. It includes information on the performance of major IT investments.

were asked about the CIO metrics and the IGs were asked about the IG metrics. Agency OCIO and IG officials were asked to denote whether each metric was “useful,” “somewhat useful,” or “not useful.” The officials were also asked to provide their reasoning for each determination. We then analyzed and summarized the responses related to the metrics agencies and their IG’s thought should be changed to better measure the effectiveness of federal agency information security programs.

Additionally, we interviewed officials from OMB, the Cybersecurity and Infrastructure Security Agency (CISA), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to discuss their role in developing FISMA metrics. We also discussed with OMB their efforts to implement recommendations from a prior FISMA-related report.

We conducted this performance audit from October 2022 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Practices Highlighted by Agencies on FISMA Implementation

The five agencies we selected for review identified various practices they had implemented to meet Federal Information Security Modernization Act of 2014 (FISMA) requirements and improve their information security posture. The following five tables summarize these practices highlighted by the selected agencies—Departments of Energy and Justice, the General Services Administration, the National Science Foundation, and the Small Business Administration.

Table 5: Practices Highlighted by Department of Energy Officials That Contribute Positively to Information Security Program Effectiveness

Practice	Agency highlighted example	Description of example
Internal communication	Chief Information Officer/Chief Information Security Officer (CIO/CISO) summit	The CIO/CISO summit is a quarterly meeting involving agency CIOs and CISOs to discuss the department's strategic direction, as well as facilitating information sharing and collaboration. Discussion topics include strategic planning, cybersecurity tools, emerging technology, contract agreements, White House priorities, executive orders, and Federal Information Security Modernization Act of 2014 (FISMA) implementation.
	Information Management Governance Board	The board is a bi-monthly forum involving CIOs and IT representatives for the collaboration, development, coordination, and execution of enterprise-wide information security activities. Specifically, these activities include enterprise-wide strategies and policies; FISMA metrics; executive orders implementation; as well as oversight and implementation of information security efforts.
	Cyber and Information Technology/Operational Technology Executive Council	The council is a quarterly forum that includes CIOs, Information Management Governance Board, and other departmental sub-groups for the collaboration and coordination of information security activities across the enterprise, as well as IT operational technology issues that require decisions by the council chair.[a] The council makes recommendations within its areas of responsibility and escalates issues as needed.
	Integrated Joint Cybersecurity Coordination Center daily operations brief	The daily operations brief includes participants from across the Department of Energy enterprise and facilitates discussions related to cyber vulnerabilities, incidents, and threat intelligence.
	Communities of practice	An example of a community of practice is a quarterly meeting of Authorizing Officials to share resources to improve cyber risk-based decisions, as well as maintain awareness of cybersecurity responsibilities. Another example is the Enterprise Cybersecurity Risk Management monthly meetings with departmental components, other agencies, and relevant service providers. The meeting includes discussions on industry standards, best practices, program updates, as well as demonstrations of tools and methodologies.

Practice	Agency highlighted example	Description of example
	Working groups	One example is the enterprise-wide Cyber Threat Intelligence working group that meets monthly to discuss vulnerabilities, incidents, and threat intelligence. Another example is the Zero Trust/Cloud working group, a bi-weekly meeting involving CISOs and information security leadership to coordinate federal zero trust and cloud requirements.[b] The Control Systems working group, consisting of departmental operational technology professionals, meets bi-monthly to collaborate on initiatives to reduce cyber risk on operational technology systems throughout the department.
Organizational culture and characteristics	Technical workforce	Department of Energy officials stated that the agency's workforce is highly technical and has effectively adapted new technology to address cybersecurity issues.

Source: GAO (analysis and data); Department of Energy (data). | GAO-24-106291

Note: Agency officials include individuals from the Office of the Chief Information Officer and Office of the Inspector General.

[a]The National Institute of Standards and Technology defines operational technology as a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.

[b]Zero trust architecture is a cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device—in contrast to traditional cybersecurity models that allow users or devices to move freely within the network once they are granted access. Zero trust works on the "never trust, always verify" principle and assumes that attacks will come from within and outside of the network.

Table 6: Practices Highlighted by Department of Justice Officials That Contribute Positively to Information Security Program Effectiveness

Practice	Agency highlighted example	Description of example
Internal communication	Chief Information Officer (CIO) council committees	The CIO council committees provide guidance and oversight on major IT domains and initiatives, as well as support for enterprise IT recommendations. Examples of these committees include the Cybersecurity Committee, Enterprise Services Committee, and the Department Investment Review Council. The Cybersecurity Committee may discuss topics such as incidents, status of recommendations, system inventory and compliance reporting, core controls, updates on department technology, or upcoming cybersecurity events. The Enterprise Services Committee may discuss data center closures, updates to program assessment procedures, updates on the implementation of new technology, or past outages. The Department Investment Review Council discusses investment reviews and provides updates on risks and challenges, investment performance, lifecycle costs, metrics, and modernization efforts.
	Department Investment Review Council	The council was established under the Department Investment Review Board to aid in oversight of Department of Justice IT programs. Its objectives are to enhance alignment and funding with department-wide strategic goals; promote performance of key IT investments; and improve effectiveness and reduce costs through component-level oversight. Specifically, the council monitors and reviews major programs against operational metrics and performance objectives. The council also advises the review board, CIO Council, and other relevant groups on program performance and assesses IT program funding requests.

Practice	Agency highlighted example	Description of example
	Security Posture Dashboard Report	This dashboard report is used to support the department's continuous monitoring program by providing real-time data on asset management, configuration management, and vulnerability management. The dashboard report is integrated with departmental information security tools and continuous monitoring processes, which enables the Office of the Chief Information Officer (OCIO) to monitor and manage systems based on risk.
	Weekly component briefs	Department of Justice officials stated that the OCIO has weekly status briefings with components to discuss remediation efforts and ensure components' compliance with department-wide requirements. These meetings also serve as a place for components to discuss upcoming data calls; progress or updates related to Federal Information Security Modernization Act of 2014 requirements; challenges, issues, or concerns; and coordination efforts.
Organizational culture and characteristics	Leadership commitment	Department of Justice officials stated that its leadership is committed to improving its cybersecurity posture and finding resources to address information security needs. Additionally, officials added that the department's leadership is well-informed of its information security status and Inspector General audit findings. According to the officials, the department's leadership emphasizes closing recommendations quickly.
Centralized policies and procedures	Department of Justice Cybersecurity Program Order	The order provides a framework for department-wide cybersecurity policy. It applies to all components, personnel, and information systems. The program is responsible for serving as the central focal point for cybersecurity; deploying and managing department-wide common security strategy; and developing and managing a comprehensive risk management program among other things. The program also defines information security and privacy requirements, methods for implementing a risk management framework, and the roles and responsibilities of relevant officials.
	Department of Justice procurement guidance document	The document outlines the processes and procedures related to acquiring IT equipment, software, and services compliant with federal law and Office of Management and Budget guidance. All Department of Justice components are expected to follow these processes and procedures when acquiring IT equipment, software, and services.
	Vulnerability Management Plan	This plan outlines the department-level framework for implementing component-level vulnerability management plans. It provides components a guide for defining and implementing vulnerability management processes.
	Information Security Continuous Monitoring Strategy	The strategy outlines the department's coordinated approach to identifying and managing security and privacy risks and complying with related requirements. According to the strategy, the department uses tools that allow for automated asset, secure configuration, and vulnerability management to maintain an ongoing awareness of its information security and privacy posture. At the organizational level, the department issued policies, procedures, and plans that define the metrics and frequencies required to implement their continuous monitoring program. At the mission level, according to the strategy, the department leverages tools, such as the dashboard report, to provide a near real-time view of their cybersecurity posture. At the system level, department system owners are responsible for implementing the policies, procedures, and plans to ensure security and privacy controls are implemented correctly.

Practice	Agency highlighted example	Description of example
	Configuration Management Plan	The plan defines the minimum processes and procedures for the configuration management of the department's information systems and assets. The plan provides guidance on configuration management activities, security and privacy considerations, minimum requirements, as well as common security configuration baselines, among other things.
	Plan of Action and Milestones Guide	The guide outlines the requirements for developing, maintaining, closing, and reporting plans of actions and milestones for all the department's IT systems and programs, including those at the component-level.
	IT Governance Guide	The IT Governance Guide describes the department's governance framework to plan and manage department- and component-level IT resources. The guide is intended to communicate procedures related to execution and oversight of the department's IT investments, programs, and initiatives to the department's stakeholders. Additionally, the guide is intended to support the achievement of IT governance goals of informing and influencing investment decisions and satisfying statutory and regulatory IT management requirements.
Audit support	FISMA audit preparation	Department of Justice officials stated that the OCIO frequently engaged with the IG. Specifically, the officials stated that OCIO coordinates with its components and the Inspector General to close recommendations. Additionally, an agency official stated that the department assesses core controls each year that are focused on upcoming Inspector General FISMA metrics.

Source: GAO (analysis and data); Department of Justice (data). | GAO-24-106291

Note: Agency officials include individuals from Office of the Chief Information Officer, Office of the Chief Information Security Officer, and Office of the Inspector General.

Table 7: Practices Highlighted by General Services Administration Officials That Contribute Positively to Information Security Program Effectiveness

Practice	Agency highlighted example	Description of example
Internal communication	Authorizing Official sync meetings[a]	The Office of the Chief Information Officer (OCIO) conducts quarterly meetings with each Authorizing Official to assess whether they are tracking threats facing their managed systems. Discussions during these meetings include updates on Office of Management and Budget memoranda and other directives, security metrics, modernization initiatives, vulnerabilities and incidents, the status of systems with authorizations to operate, and Federal Information Security Modernization Act of 2014 (FISMA) Inspector General audit findings.[b]
Organizational culture and characteristics	Leadership commitment	Agency officials stated that the culture established by senior management contributed to the General Services Administration's effective information security program ratings. According to these officials, IT senior management strives for the highest maturity levels in all FISMA metrics.
	Agency size	General Services Administration officials stated as a smaller agency they had fewer components compared to other agencies. As a result, they are able to implement technology more quickly.
	Agency mission	Agency officials stated that the agency's role in the Federal Acquisition Service allowed them to maintain awareness of and implement newer cybersecurity technology and tools.[c]

Practice	Agency highlighted example	Description of example
Centralized policies and procedures	Management Implementation Plan	Details management responsibilities and key deliverables with milestone due dates for federal- and contractor-operated systems. The plan is signed by the agency Chief Information Security Officer and every authorizing official. It documents management agreement with security milestones, activities, and measures of progress for a fiscal year. Agency officials stated that this helped set the tone for information security staff.
Audit support	Pre-audit checklists	According to agency officials, pre-audit checklists help the OCIO monitor the cyber hygiene of the agency's systems across different cybersecurity controls. These checklists contain a series of questions and items that the Office of the Inspector General will examine for the FISMA audit. These include, but are not limited to, the risk rating of systems, encryption of transmitted sensitive data, alignment with agency policy, system assessment reports, and system security plans.
	Contractor checklists	Contractor checklists are intended to assist in overseeing contractor-operated systems. When filling out the checklists, contractors must provide evidence for activities such as documentation review, contingency plan tests, incident response tests, and systems scans. The agency asks its contractors to complete the checklists on an annual or quarterly basis.
	National Institute of Standards and Technology (NIST) Cybersecurity Framework self-assessment	The General Services Administration established a self-assessment of its cybersecurity posture based on the NIST Cybersecurity Framework.[d] In completing the self-assessment, relevant officials are to identify the level they believe the agency is performing at for each framework's functional areas and provide documentation to support these self-identified levels.
	Inspector General audit meetings	According to agency officials, the OCIO exchanges information with the Office of the Inspector General on an ongoing basis through formal and informal meetings. These interactions include structured entrance and exit conferences, as well as progress meetings to discuss accomplishments, remaining work, and lessons learned. These groups also meet twice a year to review planned audits and share previous or anticipated challenges.

Source: GAO (analysis and data); General Services Administration (data). | GAO-24-106291

Note: Agency officials include individuals from Office of the Chief Information Officer, Office of the Chief Information Security Officer, Office of the Inspector General, and agency contractors.

[a]The Authorizing Official is a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

[b]An authorization to operate is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

[c]The Federal Acquisition Service is an organization within the General Services Administration that delivers products and services across the government.

[d]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (Gaithersburg, MD: Apr. 16, 2018). The Office of Management and Budget (OMB) requires Inspectors General (IG) to assess the effectiveness of information security programs on a five-level maturity model—(1) ad hoc, (2) defined, (3) consistently implemented, (4) managed and measurable, and (5) optimized. OMB considers maturity levels of four and five to be effective. However, IGs have the discretion to determine the rating of their agency's overall effectiveness or functional area at the maturity level of their choosing.

Table 8: Practices Highlighted by National Science Foundation Officials That Contribute Positively to Information Security Program Effectiveness

Practice	Agency highlighted example	Description of example
Internal communication	Daily operational meetings	The National Science Foundation organizes daily operational meetings to discuss its cybersecurity program and highlight incidents and infrastructure changes with the agency Chief Information Security Officer (CISO). These meetings typically include discussions of security alerts and the agency's response to them.
Organizational culture and characteristics	Leadership commitment	According to officials, agency leadership takes implementation of the Federal Information Security Modernization Act of 2014 (FISMA) seriously, setting an expectation to strive for high FISMA ratings. Officials stated that this type of support was helpful to them.
	Organizational model and agency size	Agency officials stated that the centralized nature of their IT security program allows them to perform consistent oversight of agency systems. Additionally, officials stated that the agency was less complex and has fewer organizations to work with internally, which made it easier to implement new technology.
Centralized policies and procedures	Information Security Handbook	The handbook provides policy and guidance to implement and maintain the National Science Foundation's IT security and privacy program consistent with federal law and guidance. It is to be used as a reference for the implementation of agency-wide IT policy, plans, and procedures.
	IT Policies, plans, and procedures	The National Science Foundation created IT-related policies, plans, and procedures that define the requirements for the agency's cybersecurity programs. The agency makes them available for system owners to reference for their programs. Examples include those related to supply chain risk management and configuration management. Additionally, the agency has developed policies and procedures for evaluating tools, documenting system authorizations, and reviewing IT external services to ensure alignment with agency and federal requirements.
Audit support	FISMA audit preparation	The National Science Foundation's cybersecurity team coordinates with the Office of Inspector General throughout the year to discuss the annual FISMA audit, open action items, and progress towards closing findings. The agency also conducts FISMA audit kickoff meetings with the Office of Inspector General and it serves as a space to discuss updates and changes to the FISMA metrics, as well as any changes in the agency's IT security program.
	Quarterly FISMA report review	The agency CISO and Chief Information Officer meet with the Office of the Inspector General quarterly to review the FISMA audit progress and discuss progress in meeting FISMA metrics. Officials stated that these activities helped demonstrate the agency's commitment in implementing information security requirements.

Source: GAO (analysis and data); National Science Foundation (data). | GAO-24-106291

Note: Agency officials include individuals from the Office of Information & Resource Management and Office of the Inspector General.

Table 9: Practices Highlighted by Small Business Administration Officials That Contribute Positively to Information Security Program Effectiveness

Practice	Agency highlighted example	Description of example
Internal communication	Weekly team lead meetings	The Information Security Division holds weekly coordination meetings with information security leads. These meetings include discussions on new or ongoing incidents, malicious activity, security tool status reports, upcoming network changes, patch management, vulnerability management, and intelligence reports from public and private partners.
	Weekly security debriefs	The Information Security Division holds weekly security debriefs with the division's branch chiefs, the Chief Information Security Officer, functional area leads, and other key staff in the Office of the Chief Information Officer (OCIO). Discussions include updates on policy and compliance, security engineering, vulnerabilities, cyber threat intelligence, penetration testing, accomplishments, security metrics, and leadership decisions.
Organizational culture and characteristics	Agency mission	An agency official stated that the public-facing nature of the agency placed privacy and cybersecurity at the forefront of the agency's efforts and awareness. Additionally, another official stated that the agency places a greater emphasis on maintaining awareness of the cybersecurity status of their systems instead of only focusing on compliance.
Centralized policies and procedures	Information Security Division policies and procedures	A division under the OCIO responsible for designing, implementing, and maturing security practices to protect critical business processes and IT assets across the agency. Among its responsibilities, the division develops and publishes the Small Business Administration Cybersecurity Policy and implementation guidance for meeting agency policy requirements. Examples of guidance that components must follow include the Small Business Administration Vulnerability Management Process and the Concept of Operations for Penetration Testing.
	New system requirements	Officials stated that system owners must adhere to specific requirements when onboarding and inventorying new systems. For example, the OCIO developed the New System Onboarding and Readiness Guidance, which defines minimum requirements for new systems. These include requirements that the new system have a vulnerability scan, penetration test, and be included in the agency's system inventory.
Shared services	Security tools	The OCIO offers information security tools for endpoint protection, identity management, network monitoring and management, email security, data security and privacy, and penetration testing, among many others. According to agency officials, the OCIO performs occasional walkthroughs of available tools to identify any gaps in their capabilities.

Source: GAO (analysis and data); Small Business Administration (data). | GAO-24-106291

Note: Agency officials include individuals from the Office of the Chief Information Officer, Office of the Chief Information Security Officer, Office of the Inspector General, and agency contractors.

Appendix III: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

December 1, 2023

Jennifer R. 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 Improve Information Security Performance Metrics" (GAO-24-106291). We have no comments.

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,

Scott Frey
Chief of Staff

Accessible Text for Appendix III: Comments from the Social Security Administration

December 1, 2023

Jennifer R. 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 Improve Information Security Performance Metrics” (GAO-24-106291). We have no comments.

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,

Scott Frey
Chief of Staff

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

December 1, 2023

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 Improve Information Security Performance Metrics (GAO-24-106291)***

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 Improve Information Security Performance Metrics* (GAO-24-106291.

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 eight of twenty-three civilian CFO Act agencies that has implemented an effective information security program as determined by the Office of Inspector General (OIG).

I am transmitting this letter from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our Information Security Performance.

Sincerely,

Colleen R. Allen

Colleen Allen
Assistant Administrator
Bureau for Management

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

December 1, 2023

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 Improve Information Security Performance Metrics (GAO-24-106291)

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 Improve Information Security Performance Metrics (GAO-24-106291.

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 eight of twenty-three civilian CFO Act agencies that has implemented an effective information security program as determined by the Office of Inspector General (OIG).

I am transmitting this letter from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our Information Security Performance.

Sincerely,

Colleen Allen
Assistant Administrator
Bureau for Management

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, Nicole Jarvis (Assistant Director), Alex Anderegg (Analyst in Charge), Amanda Andrade, Tasha Beyzavi, Chris Businsky, Garret Chan, Donna Epler, Tyler Hodges, Smith Julmisse, Ahsan Nasar, Aubrey Nguyen, and Walter Vance made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through 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