COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

Federal Information Security Modernization Act of 2014 Capstone Report, Fiscal Years 2020–2023

CIGIE Technology Committee

May 21, 2024

COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

Executive Summary, May 21, 2024

Federal Information Security Modernization Act of 2014 Capstone Report, Fiscal Years 2020–2023

Findings

Federal agencies strengthened the maturity of their information security programs on average from fiscal year (FY) 2020 through FY 2023; however, agencies should take additional steps to ensure program effectiveness. Specifically, the total percentage of agencies operating an effective information security program remained relatively stable at 60 percent from FY 2020 through FY 2023, and all cybersecurity function areas, with the exception of *identify*, increased in overall maturity governmentwide. However, within the *identify* function, inspectors general (IGs) continue to report challenges for their agencies in maturing their supply chain and cybersecurity risk management processes and controls.

From FY 2020 through FY 2023, we observed consistently higher maturity ratings by IGs for metrics in the incident response and security training domains on average, indicating that federal agencies' information security programs are stronger in these areas than they are in others. Conversely, federal agencies were consistently rated at a lower maturity by IGs, on average, for metrics in the supply chain risk management, risk management, and configuration management domains.

In addition, most of the IGs who responded to a survey issued in connection with this report indicated that they are satisfied with the CyberScope Federal Information Security Modernization Act of 2014 (FISMA) reporting application. However, respondents indicated that enhanced features related to data analytics and advanced word processing capabilities within the tool could help them meet their FISMA reporting responsibilities.

Background and Purpose

Executive Order 14028, *Improving the Nation's Cybersecurity*, states that "the United States faces persistent and increasingly malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." FISMA provides a framework for ensuring the effectiveness of information security controls and a mechanism for improved oversight of federal agencies' information security programs. Specifically, the act requires IGs to perform an annual independent evaluation to determine the effectiveness of their respective agency's information security program.

This project analyzed IG FISMA metrics reporting for FY 2020 through FY 2023 to identify trends in cybersecurity performance across the federal government. We also surveyed members of the IG community on their experiences using CyberScope, the FISMA reporting application developed and maintained by the U.S. Department of Homeland Security.

What We Did

Led by the Office of Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau, six participating OIGs analyzed governmentwide IG FISMA metrics reporting data for FY 2020 through FY 2023. Thirty-nine OIGs responded to a survey on their experiences using CyberScope.

Contents

Objective, Scope, and Methodology

The Office of Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau led this review with assistance from the OIGs for the National Science Foundation, the U.S. Department of Commerce, the U.S. Department of Defense, the U.S. Department of Homeland Security (DHS), and the U.S. Securities and Exchange Commission. This project was conducted from April 2023 through December 2023. The objective of the project was to analyze inspector general (IG) Federal Information Security Modernization Act of 2014 (FISMA) metrics reporting data for fiscal year 2020 through fiscal year 2023 to identify governmentwide trends in cybersecurity performance. The project also surveyed OIGs on their experiences using the DHS FISMA reporting application, CyberScope.[1] Note that all references to years are fiscal years, unless otherwise indicated.

To accomplish our objective, we obtained data from the CyberScope FISMA reporting tool with the assistance of DHS and the Office of Management and Budget (OMB). For anonymity, we removed agency names and stratified agencies into two types: Chief Financial Officers Act of 1990 (CFO Act) agencies and small/independent agencies.[2] The number of independent agency and commission IGs that reported FISMA metrics data during the 2020–2023 period varied. We did not include in our scope of work a determination as to why this number varied.

We performed data analyses using commercially available software on the FISMA metrics reporting data submitted by IGs across the federal government for 2020–2023 (table 1).[3]

[1] Federal agencies and IGs are required to report FISMA metrics data in the CyberScope tool.

[2] The 24 *CFO Act agencies* are the largest federal agencies subject to the act. These agencies are the U.S. Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs as well as the U.S. Agency for International Development, the U.S. Environmental Protection Agency, the U.S. General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the U.S. Nuclear Regulatory Commission, the U.S. Office of Personnel Management, the U.S. Small Business Administration, and the U.S. Social Security Administration. The *small/independent agencies* include non-CFO Act agencies and agencies that are not part of the executive branch, such as independent agencies, independent regulatory commissions, and government corporations.

[3] We did not include an analysis of IG FISMA audit, evaluation, or inspection reports prepared for 2021–2023 because (1) not all IGs prepare such reports and (2) these reports are not always publicly available. In addition, we did not include summary metrics in our analysis. Among other things, these metrics ask IGs to provide additional textual information on the effectiveness (positive or negative) of cybersecurity domains and functions, as well as of the overall program. However, we did include in our scope a determination as to how changes introduced in the scoring methodology for determining effectiveness in 2023 may have affected previous years' results.

Table 1. Summary of Agency Responses and IG FISMA Metrics Assessed for 2020–2023

Year	Number of CFO Act agencies	Number of small/ independent agencies	Total number of agencies	Number of metrics assessed
2020	24	62	86	52
2021	24	62	86	57
2022	24	60	84	20[a]
2023	24	60	84	40

Source: OIG analysis of IG FISMA results from the CyberScope FISMA reporting tool.

[a] Additional details on these 20 core metrics can be found in the Background section and in appendix A.

The number of metrics assessed by IGs can differ year to year because of changes in requirements and accompanying OMB guidance. For example, beginning in 2022, OMB introduced a cycle shift in IG FISMA reporting whereby certain high-priority metrics are to be assessed annually, with the remaining metrics assessed on a 2-year cycle. To account for these changes and enable consistent analysis,[4] we mapped, to the extent practicable,

- the 2020 metrics to the 2021 metrics[5]
- the 20 core and supplemental metrics assessed by IGs in 2022 and 2023, respectively, to the metrics in effect in 2020 and 2021[6]

We also performed a logistic regression for 2020–2022 to determine whether cybersecurity function (*identify*, *protect*, *detect*, *respond*, and *recover*) maturity ratings correlated to the IGs' overall effectiveness ratings for agency information security programs.[7]

In addition, we analyzed FISMA-related reports issued by OMB and the U.S. Government Accountability Office (GAO). Finally, we administered a survey to members of the IG community on their experiences using CyberScope. This survey gathered IG input on overall satisfaction with the CyberScope tool, awareness of tool functionality, and desired features and capabilities in CyberScope that could improve the IG FISMA reporting process. We received and analyzed 39 survey responses.

[4] Our analysis is as consistent as possible given the differing number of metrics assessed, and we note where inconsistencies make the data incomparable.

[5] The FY 2020 IG FISMA metrics did not include a domain and supporting metrics for supply chain risk management, whereas the FY 2021 IG FISMA metrics did.

[6] These core metrics were largely chosen from the metrics IGs assessed in 2020 and 2021.

[7] *Logistic regression* is a data analysis technique that is used to find the relationship between two data factors. It then uses this relationship to predict the value of one of those factors based on changes in the other.

Background

Executive Order 14028, *Improving the Nation's Cybersecurity*, states that "the United States faces persistent and increasingly malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." The SolarWinds and Microsoft Exchange security incidents underscore the importance of federal agencies developing effective, risk-based information security programs.[8] Further, GAO has listed information security as a governmentwide high-risk area since 1997, noting that cyberattacks could result in serious harm to human safety, the environment, and the economy.[9] FISMA is the key legislation outlining federal cybersecurity governance processes, program and control requirements, and reporting processes.[10]

The Federal Information Security Modernization Act of 2014

FISMA provides a framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA also establishes a mechanism for improved oversight of federal agency information security programs. Key provisions of the act include the following:

- Each agency head is required to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of
  - information collected or maintained by or on behalf of the agency.
  - information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
- Agencies are required to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

[8] As reported by GAO in *Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746, January 13, 2022, both the SolarWinds and Microsoft Exchange incidents involved foreign threat actors breaching the networks of federal agencies. The federal government confirmed that the Russian Foreign Intelligence Service infiltrated the networks at SolarWinds, whose software is widely used by federal agencies for network monitoring. The threat actor was then able to install malicious code, which was downloaded by SolarWinds' customers, including federal agencies. The Microsoft Exchange incident involved the exploitation of zero-day vulnerabilities to breach the Microsoft Exchange servers of federal agencies. A federal government official attributed this breach, with a high degree of confidence, to threat actors associated with the People's Republic of China.

[9] U.S. Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203, April 2023.

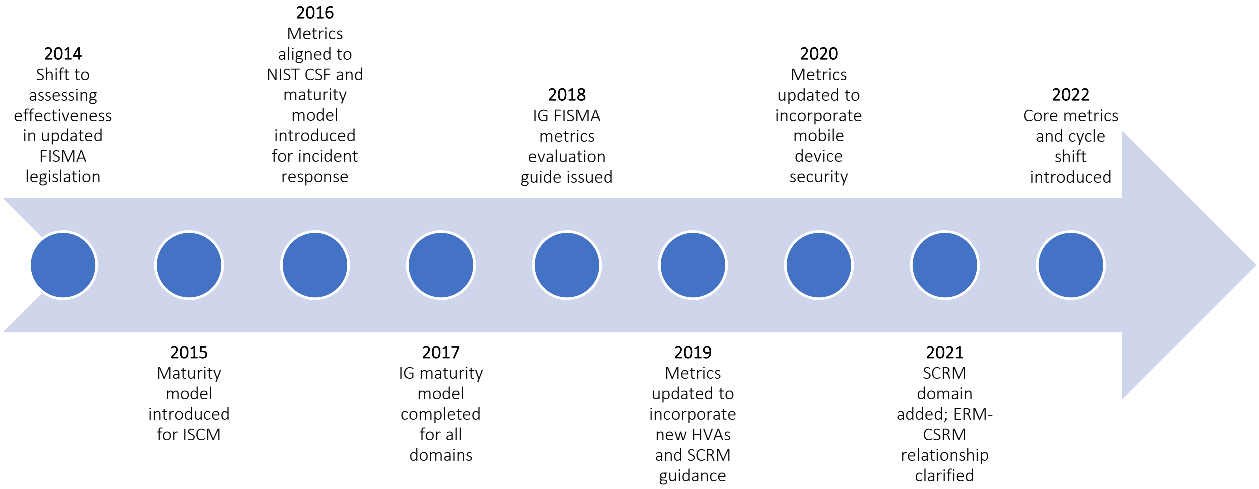
[10] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558).

- IGs are required to perform an annual independent evaluation of the information security program and practices of their respective agency to determine the effectiveness of the program and practices.[11] The IG evaluation is to include
  - testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.
  - an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.
- OMB is required to consult with DHS, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other interested parties, as appropriate, on the development of guidance for evaluating the effectiveness of an agency's information security program and practices.

Annual FISMA Reporting Guidance for IGs

OMB coordinates with CIGIE and other federal stakeholders to develop annual FISMA reporting guidance for the IG community that outlines specific cybersecurity metrics that IGs are required to assess and report on. This guidance has evolved to address a changing cybersecurity landscape (figure 1).

Figure 1. Evolution of FISMA Reporting Guidance for IGs


2014
Shift to assessing effectiveness in updated FISMA legislation
2015
Maturity model introduced for ISCM
2016
Metrics aligned to NIST CSF and maturity model introduced for incident response
2017
IG maturity model completed for all domains
2018
IG FISMA metrics evaluation guide issued
2019
Metrics updated to incorporate new HVAs and SCRM guidance
2020
Metrics updated to incorporate mobile device security
2021
SCRM domain added; ERM-CSRM relationship clarified
2022
Core metrics and cycle shift introduced

Source: OIG analysis of FISMA legislation, OMB memorandums, and IG FISMA metrics for the 2015–2022 period.

Note: Abbreviations are introduced in explanatory bullets below.

[11] The National Institute of Standards and Technology defines *security and privacy control effectiveness* as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the designated security and privacy requirements. National Institute of Standards and Technology, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, updated December 10, 2020.

The major evolutionary milestones are as follows:

- **2014: Shift to assessing effectiveness in updated FISMA legislation.** FISMA updated the Federal Information Security Management Act of 2002 (2002 Act). The key change for IGs was a new focus on effectiveness and not just on compliance. Specifically, while the 2002 Act required IGs to determine whether their respective agency complied with the law and related policies and procedures, the 2014 update added a requirement to assess whether the agency's information security program, policies, procedures, and practices are effective. This change spurred CIGIE, OMB, and other federal stakeholders to reassess how IGs were performing their annual IG FISMA evaluations, resulting in the development of a maturity model approach for assessing agencies' cybersecurity performance.
- **2015: Maturity model introduced for information security continuous monitoring (ISCM).** To better determine the effectiveness of information security programs and practices, CIGIE, in coordination with DHS, OMB, the National Institute of Standards and Technology (NIST), and other stakeholders, developed a maturity model comprising five levels: level 1 (*ad hoc*), level 2 (*defined*), level 3 (*consistently implemented*), level 4 (*managed and measurable*), and level 5 (*optimized*). Because implementing a maturity model is a large-scale undertaking, for 2015 the maturity model applied only to the ISCM area, which was an administration priority.[12] Before the maturity model was established, the IG FISMA reporting guidance largely consisted of compliance-oriented yes/no questions.[13]
- **2016: Metrics aligned to the NIST Cybersecurity Framework (CSF) and maturity model introduced for incident response.** In 2016, the IG FISMA reporting metrics were aligned to the five function areas outlined in the NIST CSF: *identify*, *protect*, *detect*, *respond*, and *recover*.[14] This alignment improved comparability with the FISMA metrics that agency chief information officers (CIOs) are required to report on. In addition, the 2016 IG FISMA reporting metrics continued the work from 2015 to develop a maturity model for the incident response area, which is another area deemed critical given the increasing threats to agency networks, systems, and data (table 2).

[12] NIST defines *ISCM* as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[13] For instance, IGs were asked questions such as whether the agency had provided security awareness training to its workforce. Without additional content, these yes/no questions made it difficult to determine effectiveness in a consistent manner.

[14] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014.

Table 2. NIST CSF Security Functions, Objectives, and Associated IG FISMA Reporting Domains

Security function	Security function objective	Associated IG FISMA reporting domain[a]
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets.	Risk management and supply chain risk management
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as to prevent, limit, or contain the impact of a cybersecurity event.	Configuration management, identity and access management, data protection and privacy, and security training
Detect	Implement activities to identify the occurrence of cybersecurity events.	Information security continuous monitoring
Respond	Implement processes to respond to a detected cybersecurity event.	Incident response
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	Contingency planning

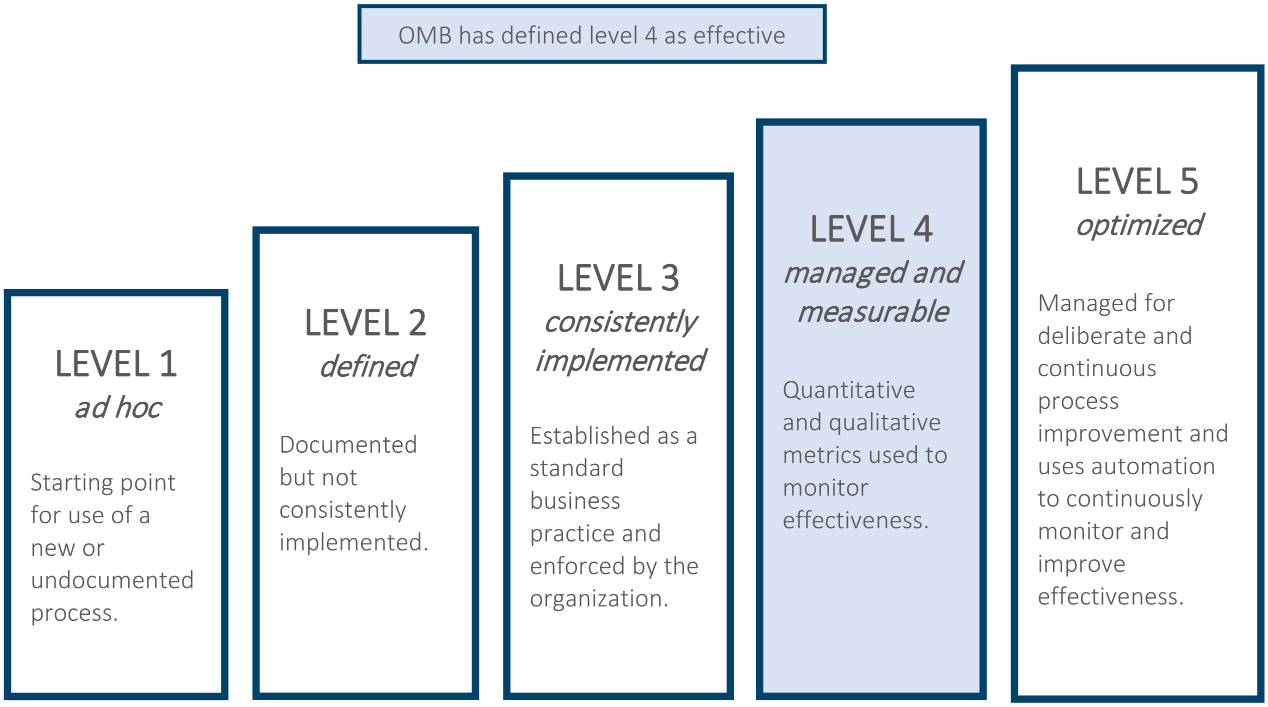
Source: OIG analysis of National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Security*, Version 1.0, February 12, 2014; and Office of Management and Budget, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1.3, September 26, 2016.

[a] This column represents the domains associated with each security function as the IG FISMA metrics exist today. The data protection and privacy and supply chain risk management domains were added to the IG FISMA metrics in 2018 and 2021, respectively.

- **2017: IG maturity model completed for all domains.** In 2017, all IG FISMA cybersecurity reporting domains transitioned to the five-level maturity model (figure 2). As of the 2024 FISMA reporting cycle, this 2017 model is used by IGs to determine the effectiveness of their respective agency's information security program. To determine the maturity of the overall information security program, IGs assess a number of metrics across the five NIST CSF function areas using this maturity model. OMB has determined that level 4 (*managed and measurable)* represents an effective level of security. IGs are encouraged and given latitude to consider their respective agency's mission, cybersecurity challenges, and available resources to address the metric challenges when determining overall effectiveness. Based on these factors, IGs may determine that their agency's information security program is operating effectively at a level other than 4. In such cases, IGs must provide a risk-based justification for their assessment.[15]

[15] For example, a small agency may justify a rating level other than 4 based on determining that the costs of a higher rating would not outweigh the benefits, given its narrow mission, relatively small budget, and less complex systems. In contrast, a large intelligence agency with a global mission and very complicated systems may decide, based on national security risks, that nothing less than an "optimized" rating is acceptable.

Figure 2. IG FISMA Maturity Model



OMB has defined level 4 as effective

LEVEL 1 *ad hoc*

Starting point for use of a new or undocumented process.

LEVEL 2 *defined*

Documented but not consistently implemented.

LEVEL 3 *consistently implemented*

Established as a standard business practice and enforced by the organization.

LEVEL 4 *managed and measurable*

Quantitative and qualitative metrics used to monitor effectiveness.

LEVEL 5 *optimized*

Managed for deliberate and continuous process improvement and uses automation to continuously monitor and improve effectiveness.

Source: OIG analysis of Office of Management and Budget, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.0, April 17, 2017.

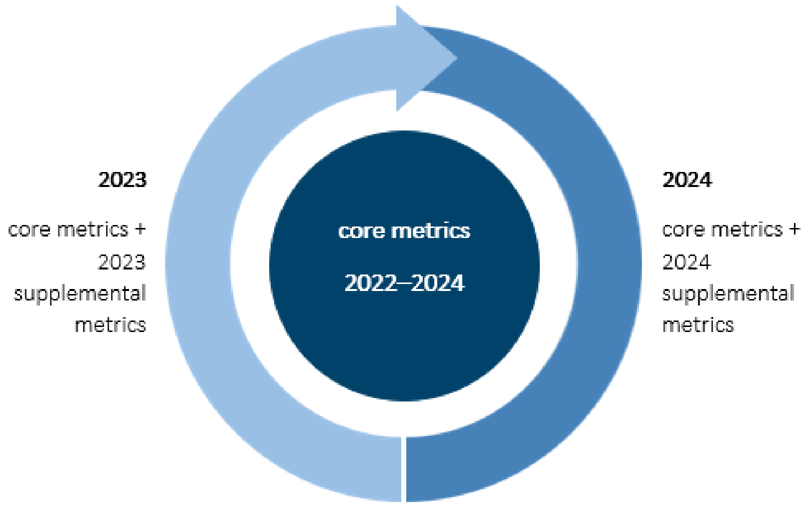
- **2018: IG FISMA metrics evaluation guide issued.** To promote consistency and comparability in IG FISMA evaluations, CIGIE, in coordination with OMB and DHS, developed an evaluation guide for IGs. The guide provides a baseline of suggested sources of evidence and types of analysis that can be used by IGs as part of their FISMA evaluations. The guide has been regularly updated to provide IGs with suggested test steps and methodologies to assess cybersecurity capabilities and determine effectiveness.
- **2019: Metrics updated to incorporate new high-value assets (HVAs) and supply chain risk management (SCRM) guidance.** In accordance with new guidance for the federal government's HVA program,[16] new metric maturity indicators and criteria references were added for IGs to evaluate agency governance and protection processes for HVAs. Further, on December 21, 2018, the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018 was passed, establishing new requirements for SCRM programs. Accordingly, the 2019 IG FISMA metrics were updated to gauge agencies' preparedness to address these new requirements while recognizing that specific guidance would be issued at a later date.
- **2020: Metrics updated to incorporate mobile device security.** In 2020, the administration increased its focus on the security of mobile devices (government-furnished equipment and nongovernment-furnished equipment), particularly in the areas of mobile device management

[16] Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, OMB Memorandum M-19-03, December 10, 2018.

and enterprise mobility management. As such, the 2020 IG FISMA metrics were updated to require IGs to assess agency processes for securing mobile endpoints and employing secure application development processes.

- **2021: SCRM domain added; enterprise risk management (ERM)—cybersecurity risk management (CSRM) relationship clarified.** In 2021, increasing the maturity of the federal government's SCRM programs was, and continues to be, an administration priority. As such, a new domain within the *identify* function area was added for IGs to assess the maturity of agency SCRM strategies, policies and procedures, and plans. In addition, specific metrics within the *identify* function were clarified to focus on the extent to which CSRM and ERM processes are integrated.
- **2022: Core metrics and cycle shift introduced.** In 2022, OMB introduced a cycle shift that has certain core metrics evaluated annually and the remaining metrics (supplemental) evaluated over a 2-year period (figure 3). Specifically, starting in 2022, core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness. Beginning in 2023, half of the supplemental metrics were to be assessed in 2023 and the other half in 2024. Supplemental metrics represent important activities conducted by security programs that contribute to the overall evaluation and determination of security program effectiveness. The core metrics are described in appendix A.

Figure 3. Cycle Shift in IG FISMA Reporting, 2022–2024


2023
core metrics + 2023 supplemental metrics
core metrics
2022–2024
2024
core metrics + 2024 supplemental metrics

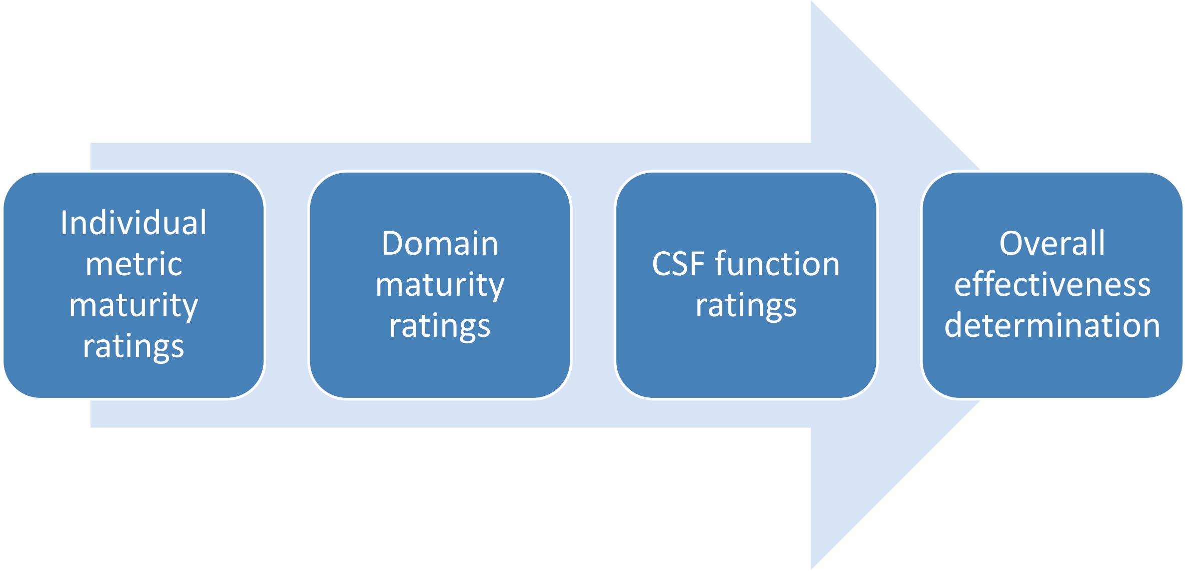
Source: OIG analysis of Office of Management and Budget, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-22-05, December 6, 2021.

Determining the Effectiveness of Agency Information Security Programs

To determine whether an agency's information security program is effective, IGs consider the maturity ratings of individual metrics, domains, and function areas (figure 4). Specifically,

- IGs assign a maturity level to each cybersecurity metric. Appendix B provides a breakdown of the number of metrics assessed by IGs by domain and CSF function area.
- These metric-level ratings inform the domain-level maturity (for example, risk management and configuration management).
- The domain-level ratings inform the CSF function-level maturity ratings (meaning, *identify*, *protect*, *detect*, *respond*, and *recover*).
- The CSF function-level maturity ratings inform the IG's overall determination of the effectiveness of the agency's information security program.

Figure 4. Key Components of IG Effectiveness Determinations of Agency Information Security Programs


Individual metric maturity ratings
Domain maturity ratings
CSF function ratings
Overall effectiveness determination

Source: OIG analysis of Office of Management and Budget, *FY 2023–FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, February 10, 2023.

Scoring Methodology

Historically, IGs have been directed to determine maturity using a mode-based approach in which the most frequent level assigned across the metrics serves as the domain rating. For example, if there are seven questions in a domain, and the agency receives *defined* ratings for three questions and *managed and measurable* ratings for four questions, then the domain rating is *managed and measurable*. Similarly, IGs have historically been encouraged to use the domain ratings to inform the overall function ratings and to use the five function ratings to inform the overall agency rating, both of which are calculated using the mode. IGs continue to have discretion to determine the overall effectiveness rating and the rating for each of the CSF functions at the maturity level of their choosing based on agency-specific risk factors, such as unique missions, risk environments, and resources available.[17]

[17] U.S. Department of Homeland Security, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

Beginning with the 2023 IG FISMA reporting process, IG scoring transitioned to a more risk-based approach using a calculated average.[18] In addition, to provide IGs with additional flexibility and encourage evaluations based on agencies' risk tolerance and threat models, calculated averages are not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, IGs are encouraged to focus on the results of the core metrics, as these tie directly to administration priorities and other high-risk areas. IGs should use the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program- and function-level effectiveness. Further, IGs should consider additional factors, such as the results of cybersecurity reviews conducted during the review period, the progress made by agencies in addressing IG recommendations, and reported security incidents during the review period. For example, if the calculated average of all the core metrics is 3.4 and all the supplemental metrics are 3.7, an IG may decide that the overall program is effective because of the higher supplemental average and based on progress made in addressing outstanding weaknesses.

[18] By analyzing prior years' IG FISMA reporting data, OMB and CIGIE determined that a calculated average aligned more closely with IGs' assessed maturity levels than a mode-based approach. With the calculated average approach, IGs are directed to take an average of the five function-level ratings to determine overall program effectiveness.

Results of Review

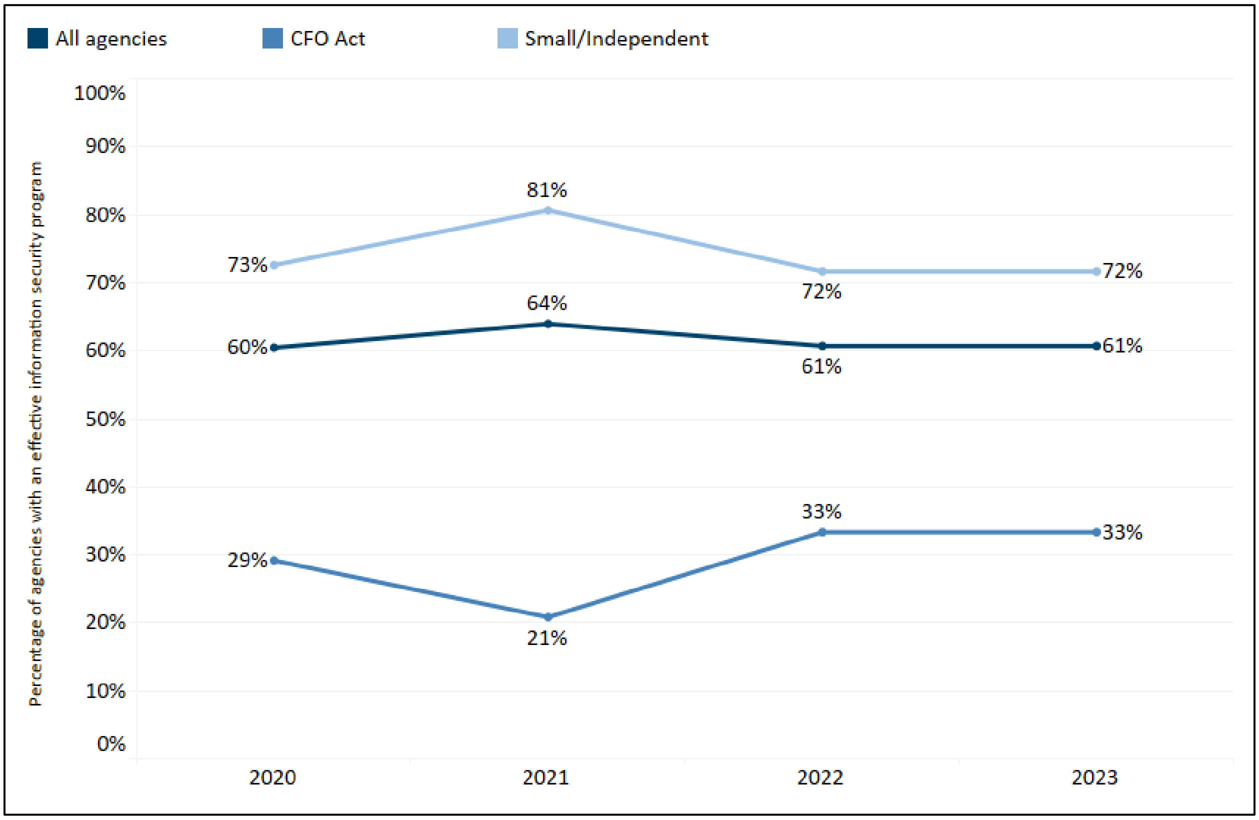
Overall, we found that federal agencies made progress in maturing their information security programs during the 2020–2023 period. The incident response and security training domains of agencies' information security programs were areas of strength compared with the other domains. In addition, federal agencies on average have increased their maturity scores for 18 of the 20 core metrics during the 2020–2023 period.

However, we found that federal agency information security programs on average are not as mature in the SCRM, risk management, and configuration management domains. Further, we found that while IGs are generally satisfied with CyberScope, additional functionality for data analytics and advanced word processing capabilities would help IGs meet their FISMA reporting responsibilities.

Information Security Program Effectiveness

From 2020 through 2023, federal agencies continued to make progress in maturing their information security programs (figure 5).

Figure 5. Trends in Information Security Program Effectiveness, 2020–2023



Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Specifically, we observed the following for the 2020–2023 period:

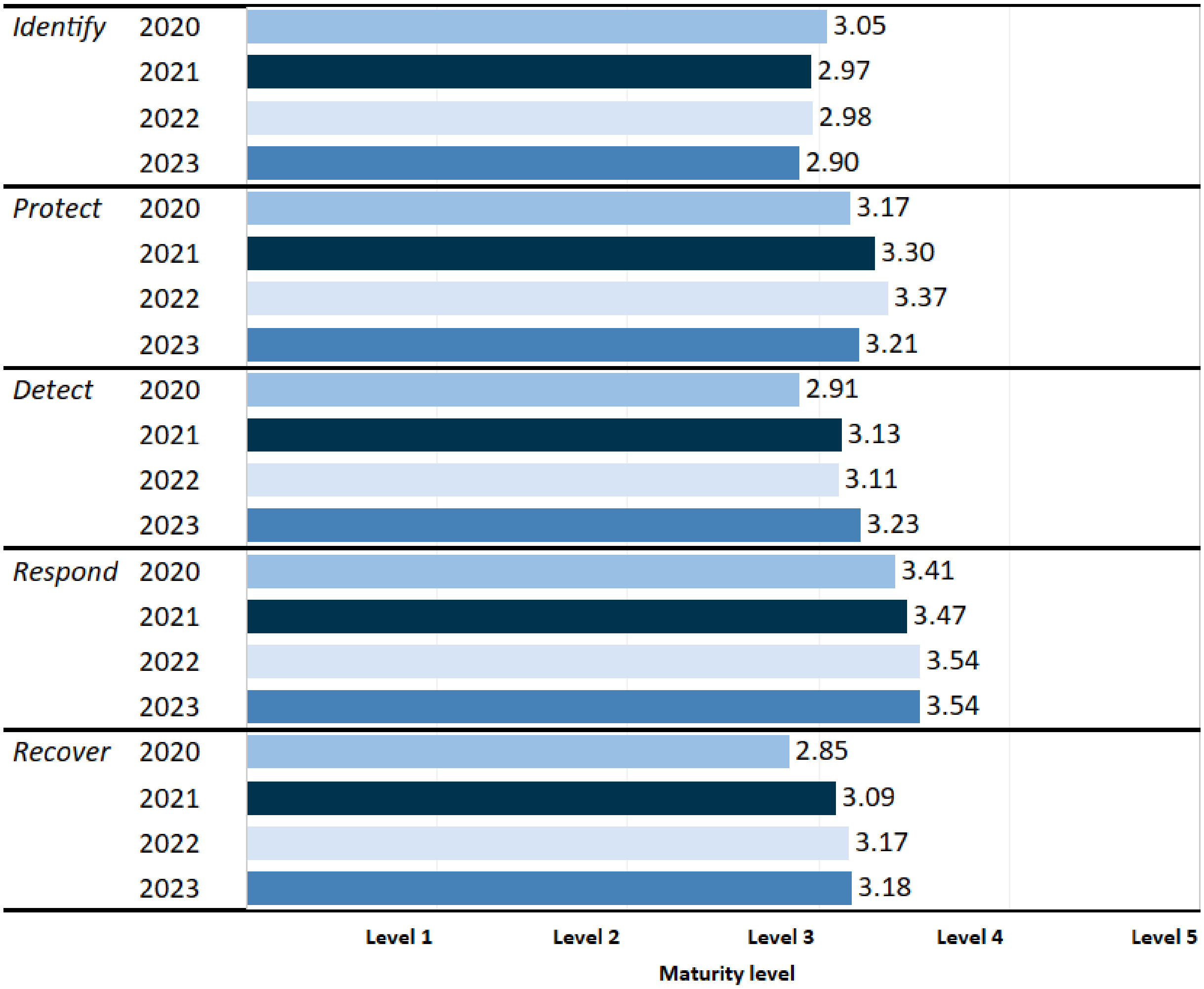
- The percentage of federal agencies (CFO Act agencies and small/independent agencies) that were rated by their IGs as having an effective information security program remained relatively constant at approximately 60 percent.
- The number of CFO Act agencies with information security programs rated as effective by their IGs was approximately 4 percent higher in 2023 than in 2020.
- CFO Act agencies experienced a 12 percent increase in effectiveness ratings from 2021 to 2022, whereas small/independent agencies' effectiveness ratings decreased by 9 percent during that same period. As noted, starting in 2022 IG effectiveness determinations have been largely based on the 20 core metrics, which changed CFO Act agency and small/independent agency effectiveness ratings. The overall governmentwide average remained relatively constant at approximately 60 percent.
- On average, information security program effectiveness at small/independent agencies is approximately 45 percent higher than at CFO Act agencies.[19]

CSF Function-Level Effectiveness

From 2020 through 2023, federal agencies continued to mature their information security programs at the CSF function level (figures 6 and 7).

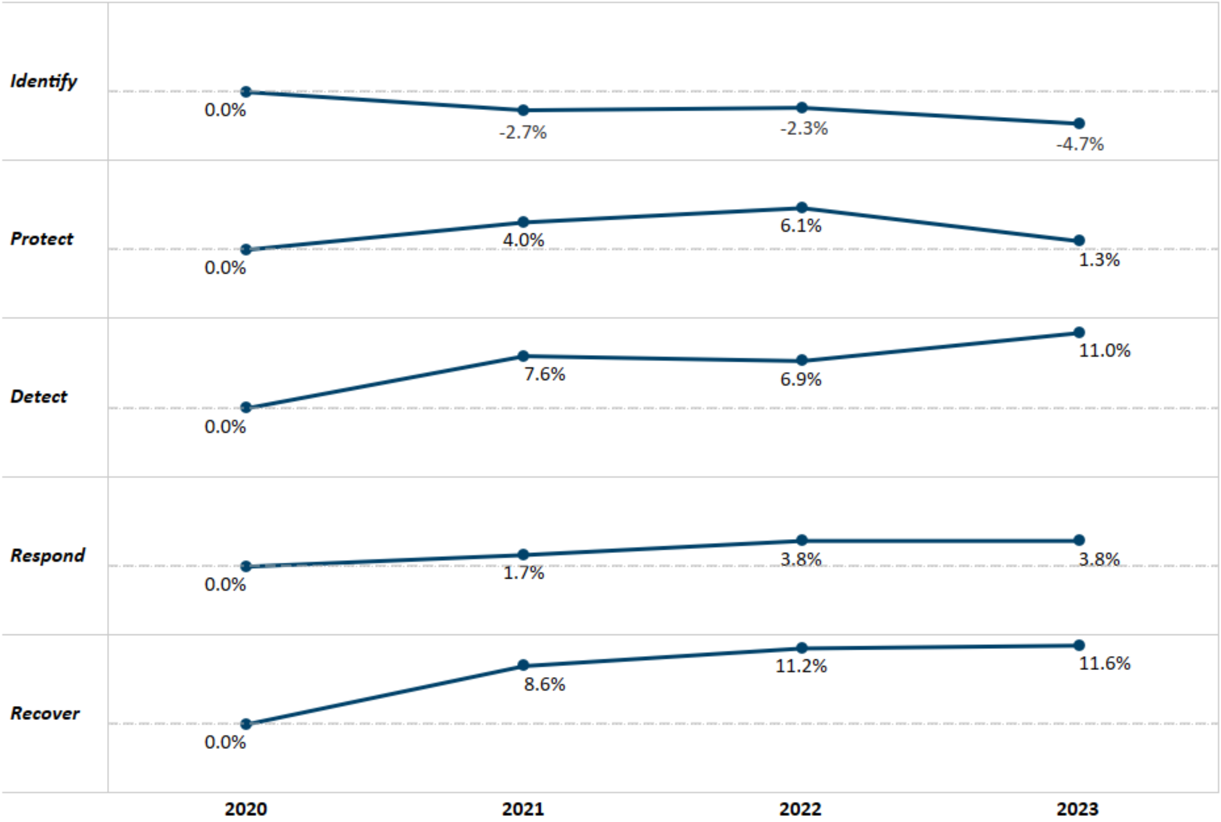
[19] While this review did not determine the causes of these differences, we believe that because CFO Act agencies are large and often comprise multiple operating divisions or bureaus, it may be more difficult for them to implement FISMA programs, processes, and controls agencywide as compared to small/independent agencies. However, because of the size, mission, and complexity of CFO Act agencies, we believe it is crucial that their information security programs are effective.

Figure 6. Trends in CSF Function-Level Effectiveness, All Agencies, 2020–2023



Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Figure 7. Percentage Change in CSF Function-Level Effectiveness, All Agencies, 2020–2023



Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Specifically, we observed the following for the 2020–2023 period:

- For all agencies, all CSF function areas except *identify* increased in overall maturity. Specifically, the maturity ratings increased as follows: *recover*, 11.6 percent; *detect*, 11.0 percent; *respond*, 3.8 percent; and *protect*, 1.3 percent. Conversely, the maturity ratings for the *identify* function decreased by 4.7 percent. We believe that the *identify* function ratings decreased because IGs continue to identify challenges faced by their agencies in maturing their SCRM and CSRM processes.
- The *respond* function is the closest to approaching an overall effective level (level 4, *managed and measurable*) across the federal government. Although the *respond* function was the highest rated on average, all five function areas are operating at level 3 (*consistently implemented*) (table 3).

Table 3. Average CSF Function-Level Maturity Ratings, All Agencies, 2020–2023

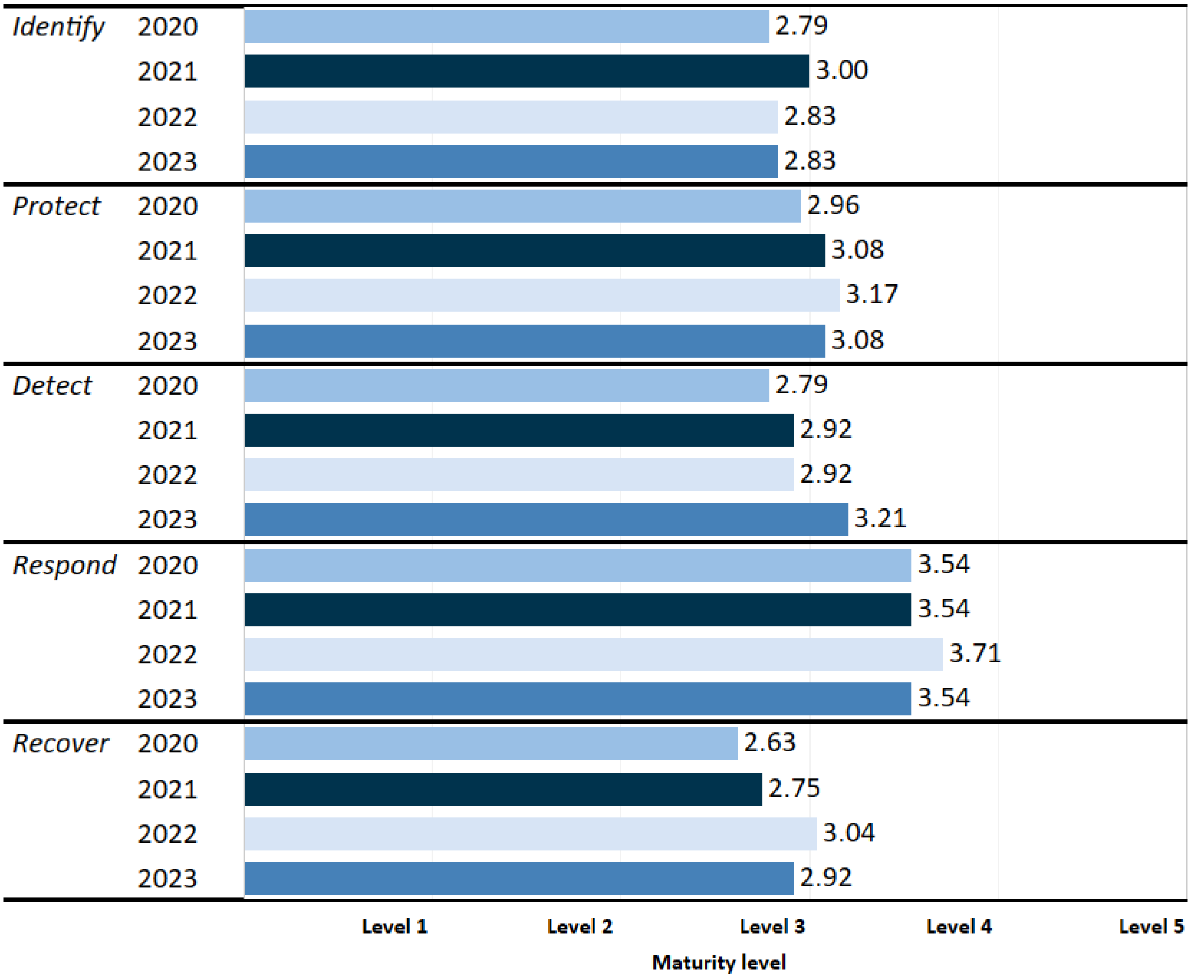
Security function	Average maturity rating	Associated maturity level
Identify	2.98	Level 3 (*consistently implemented*)
Protect	3.26	Level 3 (*consistently implemented*)
Detect	3.09	Level 3 (*consistently implemented*)
Respond	3.49	Level 3 (*consistently implemented*)
Recover	3.07	Level 3 (*consistently implemented*)

Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Note: Scores of 0.49 and lower are rounded down to the lower maturity level; scores of 0.50 and higher are rounded up to the next maturity level.

- We observed slightly different trends for CFO Act agencies during the 2020–2023 period; the maturity ratings for each of the function areas fluctuated during the period, but when comparing 2020 to 2023, they all either increased or remained the same (figure 8).

Figure 8. Trends in CSF Function-Level Effectiveness, CFO Act Agencies, 2020–2023



Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

On average, CFO Act agencies are rated effective overall in the *respond* function area (table 4).

Table 4. Average CSF Function-Level Maturity Ratings, CFO Act Agencies, 2020–2023

Security function	Average maturity rating	Associated maturity level
Identify	2.86	Level 3 (*consistently implemented*)
Protect	3.07	Level 3 (*consistently implemented*)
Detect	2.96	Level 3 (*consistently implemented*)
Respond	3.58	Level 4 (*managed and measurable*)
Recover	2.83	Level 3 (*consistently implemented*)

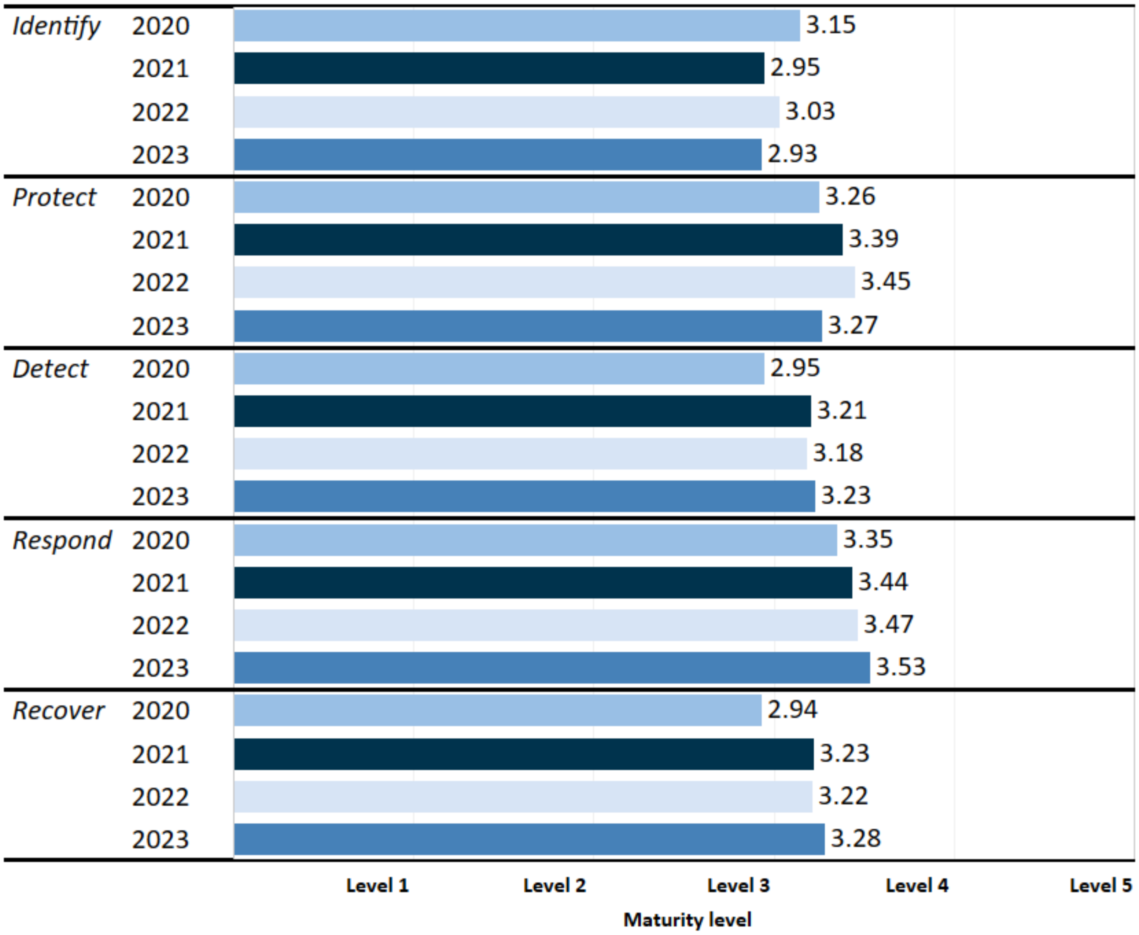
Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Note: Scores of 0.49 and lower are rounded down to the lower maturity level; scores of 0.50 and higher are rounded up to the next maturity level.

We observed the following for small/independent agencies during the 2020–2023 period:

- The maturity ratings for each of the function areas fluctuated during the period, but when comparing 2020 to 2023, they all, with the exception of *identify*, either increased or remained the same (figure 9).

Figure 9. Trends in CSF Function-Level Effectiveness, Small/Independent Agencies, 2020–2023



Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

- On average, small/independent agencies are rated at level 3 (*consistently implemented*) for all five function areas (table 5).
- With the exception of the *respond* function, on average, small/independent agency function-level scores were higher than those of CFO Act agencies by approximately 5 percent.

Table 5. Average CSF Function-Level Maturity Ratings, Small/Independent Agencies, 2020–2023

Security function	Average maturity rating	Associated maturity level
Identify	3.02	Level 3 (*consistently implemented*)
Protect	3.34	Level 3 (*consistently implemented*)
Detect	3.14	Level 3 (*consistently implemented*)
Respond	3.45	Level 3 (*consistently implemented*)
Recover	3.16	Level 3 (*consistently implemented*)

Source: OIG analysis of IG FISMA metric results for the 2020–2023 period.

Note: Scores of 0.49 and lower are rounded down to the lower maturity level; scores of 0.50 and higher are rounded up to the next maturity level.

Top 10– and Bottom 10–Rated Metrics

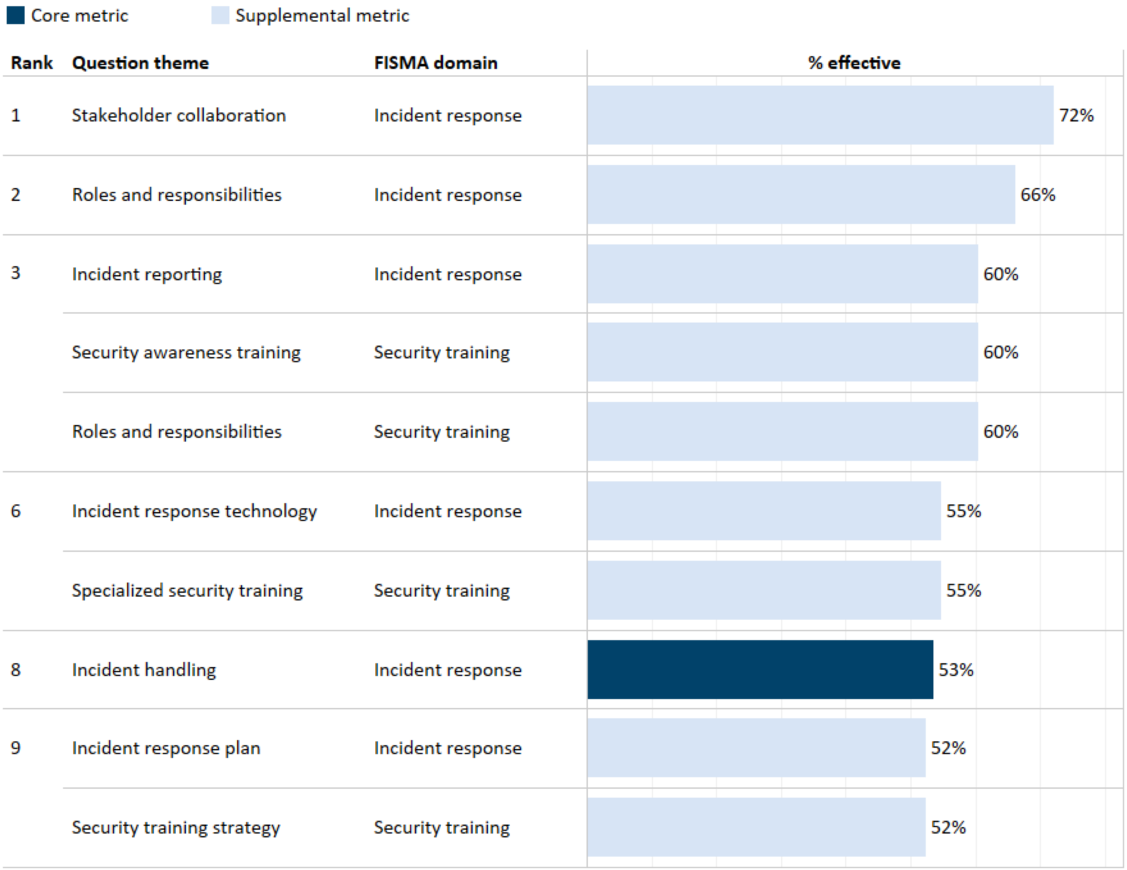
For 2021 and 2023, we analyzed the top 10– and bottom 10–rated FISMA metrics by IGs for all agencies (figures 10–13).[20] We identified the following:

- In both 2021 and 2023 the majority of the top 10–rated metrics were within the incident response and security training domains, indicating that federal agencies' information security programs were stronger in these areas than in others. For instance, in 2021, all metrics within the top 10 were in the incident response and security training domains, and none of the metrics in the bottom 10 were in these domains. We also observed that for 2023, federal agencies made progress in improving their ratings in the risk management domain, with metrics related to system inventory and asset management appearing in the top 10.
- In 2021, the majority of the bottom 10–rated metrics were within the risk and configuration management domains, indicating that federal agencies' information security programs were less effective in these areas as compared to others. For instance, in 2021 over half of the bottom 10-rated metrics were in the risk and configuration management domains.
- In 2023, we observed slightly different trends with respect to the bottom 10–rated metrics. While configuration settings and flaw remediation were still among the bottom 10, the metrics with the

[20] The top 10 and bottom 10 analysis focused on 2021 and 2023 because (1) 2021 was the last year in our sample in which all the metrics were assessed by the IGs (meaning, before the cycle shift) and (2) in 2023, IGs were required to evaluate the core metrics and half of the supplemental metrics, both of which were chosen from the metrics in 2021. In 2022, IGs were only required to evaluate the core metrics.

lowest maturity, or effectiveness, ratings were in the SCRM domain. These metrics are for SCRM strategies, policies, procedures, and processes for third-party security. As noted above, SCRM was added to the IG FISMA metrics in 2021 as a new domain within the *identify* function area. However, to provide agencies with sufficient time to fully implement the SCRM requirements outlined in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*, the SCRM metrics were not considered for the purposes of determining effectiveness ratings until 2022.

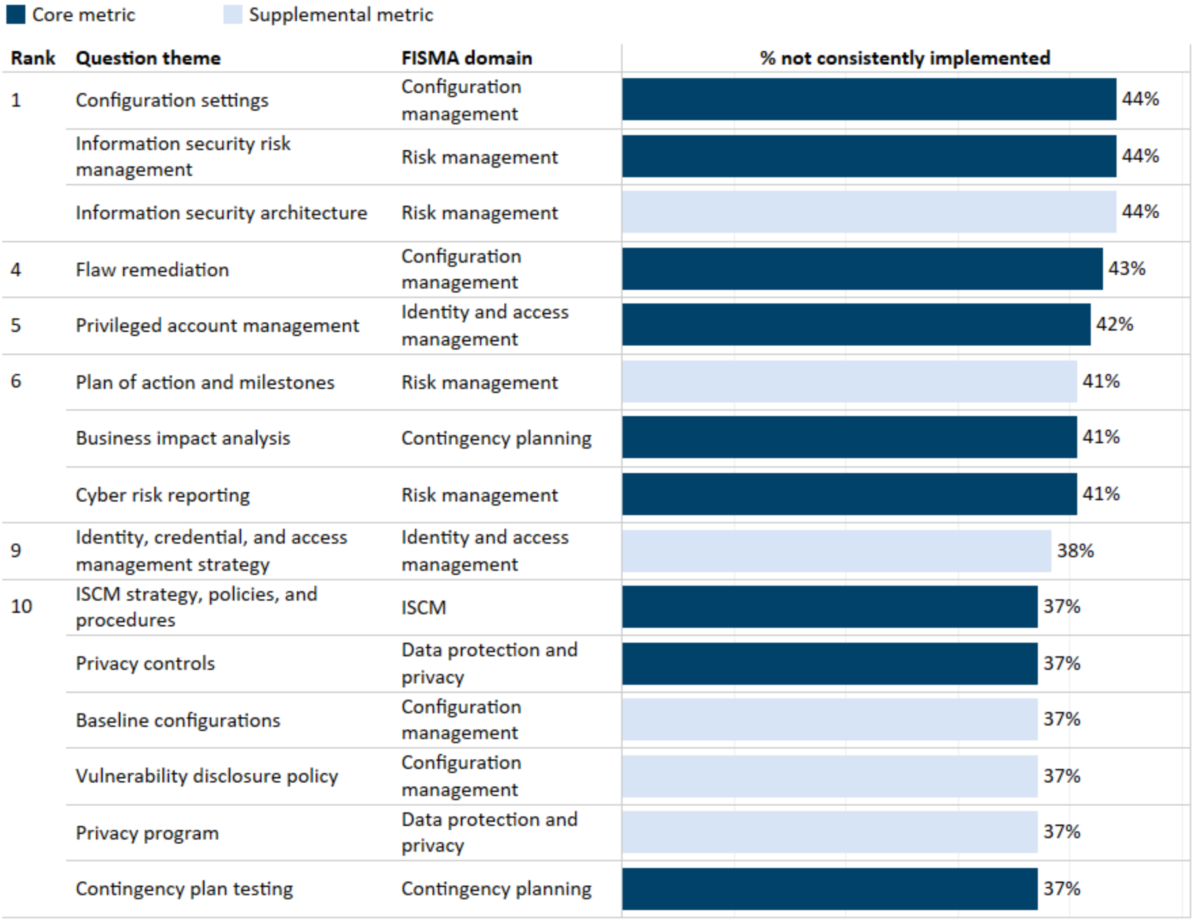
Figure 10. Top 10–Rated IG FISMA Metrics for 2021



Source: OIG analysis of IG FISMA metric results for 2021.

Note: *% effective* refers to those metrics rated at level 4 (*managed and measurable*) or level 5 (*optimized*).

Figure 11. Bottom 10–Rated IG FISMA Metrics for 2021



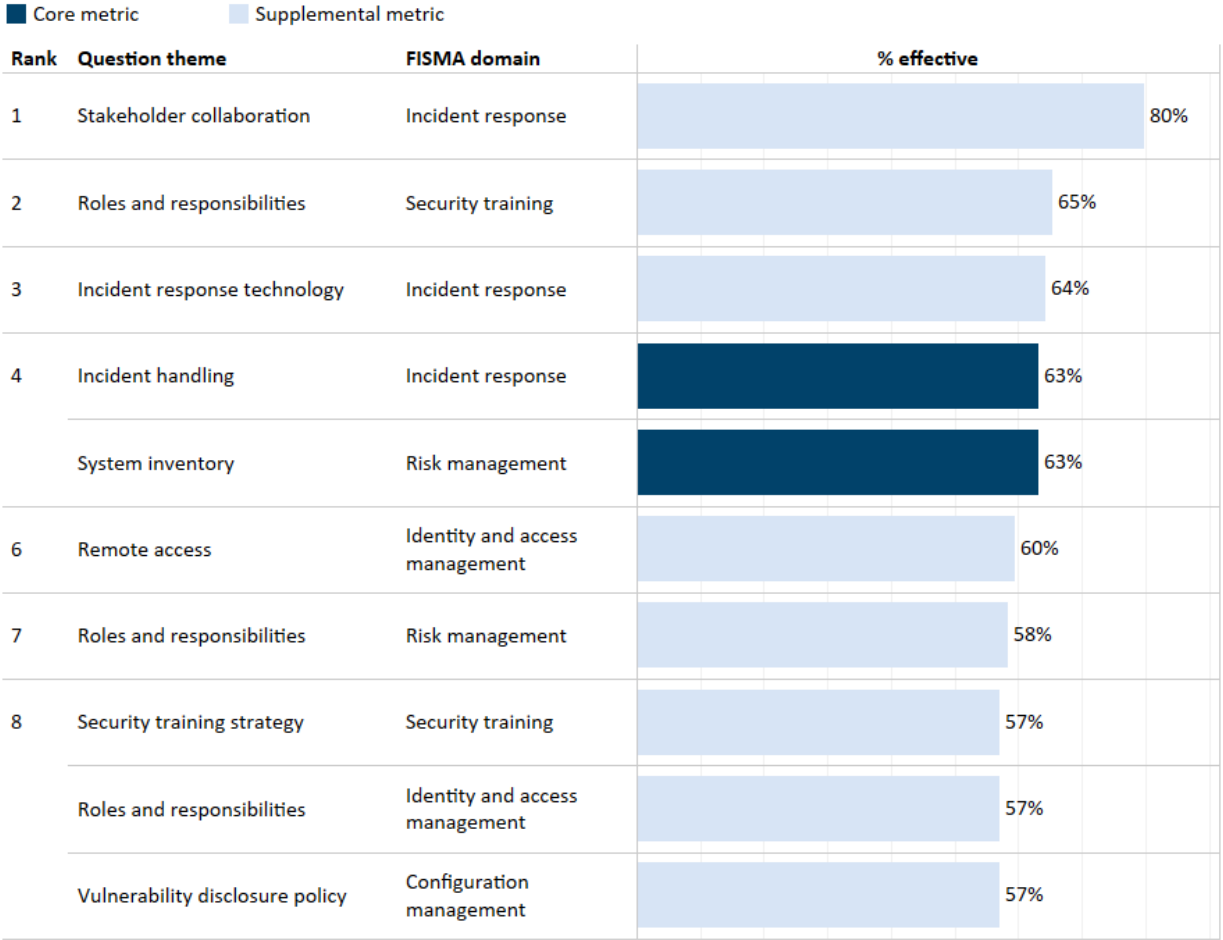
■ Core metric □ Supplemental metric

Rank	Question theme	FISMA domain	% not consistently implemented
1	Configuration settings	Configuration management	■ 44%
	Information security risk management	Risk management	■ 44%
	Information security architecture	Risk management	□ 44%
4	Flaw remediation	Configuration management	■ 43%
5	Privileged account management	Identity and access management	■ 42%
6	Plan of action and milestones	Risk management	□ 41%
	Business impact analysis	Contingency planning	■ 41%
	Cyber risk reporting	Risk management	■ 41%
9	Identity, credential, and access management strategy	Identity and access management	□ 38%
10	ISCM strategy, policies, and procedures	ISCM	■ 37%
	Privacy controls	Data protection and privacy	■ 37%
	Baseline configurations	Configuration management	□ 37%
	Vulnerability disclosure policy	Configuration management	□ 37%
	Privacy program	Data protection and privacy	□ 37%
	Contingency plan testing	Contingency planning	■ 37%

Source: OIG analysis of IG FISMA metric results for 2021.

Note: *% not consistently implemented* refers to those metrics rated at level 2 (*defined*) or level 1 (*ad hoc*).

Figure 12. Top 10–Rated IG FISMA Metrics for 2023[a]

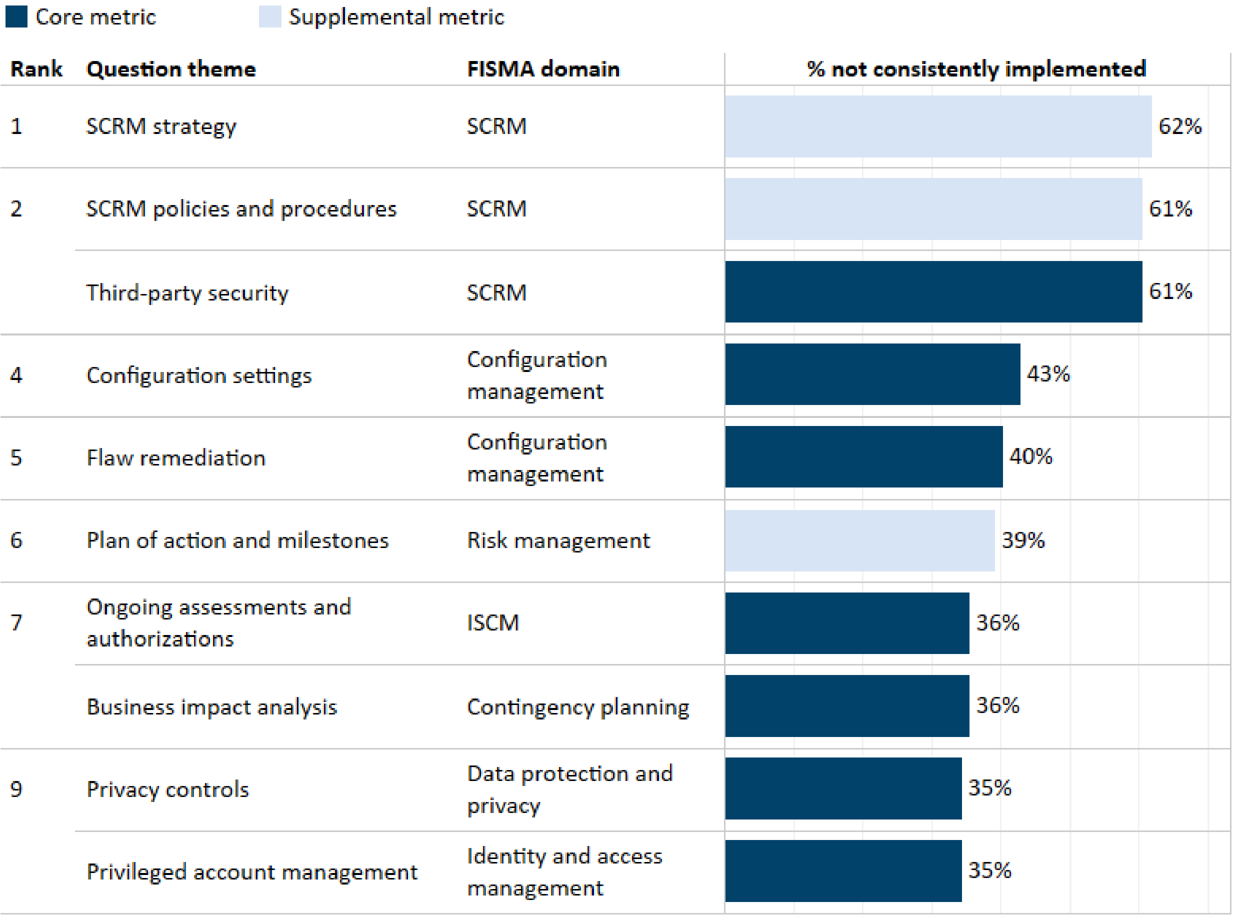


Rank	Question theme	FISMA domain	% effective
1	Stakeholder collaboration	Incident response	80%
2	Roles and responsibilities	Security training	65%
3	Incident response technology	Incident response	64%
4	Incident handling	Incident response	63%
	System inventory	Risk management	63%
6	Remote access	Identity and access management	60%
7	Roles and responsibilities	Risk management	58%
8	Security training strategy	Security training	57%
	Roles and responsibilities	Identity and access management	57%
	Vulnerability disclosure policy	Configuration management	57%

Source: OIG analysis of IG FISMA metric results for 2023.

Note: *% effective* refers to those metrics rated at level 4 (*managed and measurable*) or level 5 (*optimized*).

Figure 13. Bottom 10–Rated IG FISMA Metrics for 2023



■ Core metric □ Supplemental metric

Rank	Question theme	FISMA domain	% not consistently implemented
1	SCRM strategy	SCRM	□ 62%
2	SCRM policies and procedures	SCRM	□ 61%
	Third-party security	SCRM	■ 61%
4	Configuration settings	Configuration management	■ 43%
5	Flaw remediation	Configuration management	■ 40%
6	Plan of action and milestones	Risk management	□ 39%
7	Ongoing assessments and authorizations	ISCM	■ 36%
	Business impact analysis	Contingency planning	■ 36%
9	Privacy controls	Data protection and privacy	■ 35%
	Privileged account management	Identity and access management	■ 35%

Source: OIG analysis of IG FISMA metric results for 2023.

Note: *% not consistently implemented* refers to those metrics rated at level 2 (*defined*) or level 1 (*ad hoc*).

These results are similar to those noted in other governmentwide cybersecurity reports issued by OMB and GAO. For example, in its fiscal year 2021 FISMA report to Congress, OMB noted that the most commonly identified security deficiencies related to HVAs are for configuration management. Specifically, the top five HVA assessment findings in 2021 are for patch management, cleartext protocols, unsupported SSL/TLS (secure socket layer/transport layer security) encryption ciphers, database configuration, and insecure default configuration. The report also notes that the federal government faces challenges in the growing scale and complexity of securing the information technology supply chain. Further, the report emphasizes that "when Federal agencies have effective cybersecurity risk management, they are better able to protect information systems and ensure they can continue their core missions serving the American people."[21]

In its fiscal year 2022 FISMA report to Congress, OMB also noted that the top five HVA assessment findings were for the five configuration management–related areas found in 2021. OMB also noted that

[21] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2021*, September 14, 2022.

agencies are well positioned to respond to incidents, noting that "every agency worked to evaluate CISA's [Cybersecurity and Infrastructure Security Agency] Cybersecurity Incident and Vulnerability Response Playbooks against their current IR [incident response] procedures and determined a process for sharing incident details electronically with CISA."[22] These results are in line with IG FISMA results for the 2020–2023 period, showing that while specific incident response metrics and the *respond* function overall are among the highest rated, configuration management—namely, configuration settings and flaw remediation—continue to be among the lowest-rated metrics in terms of effectiveness.

Similarly, in 2019 GAO noted that to protect against cyber threats, federal agencies need to strengthen their cyber risk management programs in, among other areas, risk management strategy and policies, assessing cyber risks, and coordinating between cybersecurity and ERM functions.[23] Further, subsequent GAO reviews have identified weaknesses in access controls, configuration management, and the protection of data shared with external entities.[24]

Core Metrics Analysis

As noted earlier, OMB introduced a cycle shift for the 2022–2024 IG FISMA reporting process in which certain core metrics are evaluated annually and the remaining supplemental metrics are evaluated over a 2-year period. Core metrics represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness. From 2021 through 2023, federal agencies continued to make progress in maturing their information security programs in the core metric areas (figure 14).[25]

[22] Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report Fiscal Year 2022*, May 1, 2023.

[23] U.S. Government Accountability Office, *Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384, July 25, 2019.

[24] U.S. Government Accountability Office, *Cybersecurity: Preliminary Results Show That Agencies' Implementation of FISMA Requirements Was Inconsistent*, GAO-22-105637, January 11, 2022.

[25] The core metrics applicable for the 2022–2024 reporting period were chosen from the 2021 IG FISMA reporting metrics. As such, while the 2021 IG FISMA reporting process did not include core metrics, we are able to map the core metrics and report on trends.

Figure 14. Average Core Metrics Ratings, All Agencies, 2021–2023

FISMA domain	Question theme	2021	2022	2023	% change
Risk management	System inventory	3.35	3.54	3.56	6%
	Hardware asset management	3.19	3.20	3.42	7%
	Software asset management	3.16	3.15	3.42	8%
	Information security risk management	2.86	2.92	3.24	13%
	Cyber risk reporting	2.71	3.04	3.30	22%
SCRM	Third-party security	1.66	1.99	2.31	39%
Configuration management	Configuration settings	2.90	3.00	3.07	6%
	Flaw remediation	2.88	2.86	3.07	7%
Identity and access management	Multifactor authentication (nonprivileged users)	3.23	3.32	3.36	4%
	Multifactor authentication (privileged users)	3.20	3.30	3.37	5%
	Privileged account management	2.83	2.88	2.99	6%
Data protection and privacy	Privacy controls	2.97	2.96	3.08	4%
	Enhanced network protections	3.20	3.23	3.37	5%
Security training	Cyber workforce assessment	3.26	3.24	3.37	3%
ISCM	ISCM strategy, policies, and procedures	2.97	2.99	3.30	11%
	Ongoing assessments and authorizations	3.16	3.05	3.15	0%
Incident response	Incident detection and analysis	3.27	3.33	3.06	-6%
	Incident handling	3.50	3.46	3.63	4%
Contingency planning	Business impact analysis	2.79	2.89	3.04	9%
	Contingency plan testing	2.88	2.87	3.00	4%

Source: OIG analysis of IG FISMA metric results for the 2021–2023 period.

Note: The % change reflects the difference between the 2021 and 2023 average maturity.

Our analysis of the core metrics identified the following:

- From 2021 through 2023, the average maturity ratings for all agencies increased for 18 of the 20 core metrics. The core metrics showing the greatest increase were in the SCRM and risk management domains. Incident detection and analysis exhibited a 6 percent decline in average maturity, and the average maturity rating for ongoing assessments and authorizations declined by 0.1 percent.
- From 2021 through 2023, the core metric for SCRM (third-party security) scored the lowest. While scores for this core metric increased from 2021 to 2023 (by approximately 20 percent from 2021 to 2022 and by approximately 16 percent from 2022 to 2023), this metric was the only core metric at an average level 2 (*defined*) maturity across the federal government.

In addition, we analyzed the lowest-ranked core metrics and identified the following (table 6):

- In 2021 and 2022, the lowest-ranked core metrics remained the same but shifted somewhat in ranking. These metrics and their associated NIST CSF functions and cyber domains are as follows:
    - information security risk management (*identify*, risk management)
    - cyber risk reporting (*identify*, risk management)
    - third-party security (*identify*, SCRM)
    - configuration settings (*protect*, configuration management)
    - flaw remediation (*protect*, configuration management)
    - privileged account management (*protect*, identity and access management)
    - privacy controls (*protect*, data protection and privacy)
    - ISCM strategy, policies, and procedures (*detect*, ISCM)
    - contingency plan testing (*recover*, contingency planning)
    - business impact analysis (*recover*, contingency planning)

Table 6. Lowest-Ranked Core Metrics, All Agencies, 2021–2023

Ranking (lowest to highest)	2021	2022	2023
1	Third-party security	Third-party security	Third-party security
2	Cyber risk reporting	Flaw remediation	Privileged account management
3	Business impact analysis	Contingency plan testing	Contingency plan testing
4	Privileged account management	Privileged account management	Business impact analysis
5	Information security risk management	Business impact analysis	Incident detection and analysis
6	Contingency plan testing	Information security risk management	Configuration settings
7	Flaw remediation	Privacy controls	Flaw remediation
8	Configuration settings	ISCM strategy, policies, and procedures	Privacy controls
9	ISCM strategy, policies, and procedures	Configuration settings	Ongoing assessments and authorizations
10	Privacy controls	Cyber risk reporting	Information security risk management

Source: OIG analysis of the 10 lowest-ranked IG FISMA core metrics for the 2021–2023 period.

Note: Shading indicates NIST CSF function:

🟦 *identify* ⬜ *protect* 🟨 *detect* 🟩 *respond* 🟧 *recover*

- From 2022 to 2023, the lowest-ranked core metrics remained largely the same, with two exceptions:
  - Agency performance on cyber risk reporting (*identify*, risk management) and ISCM strategy, policies, and procedures (*detect*, ISCM) improved, moving these core metrics out of the bottom 10.
  - Agency performance on ongoing assessments and authorizations (*detect*, ISCM) and incident detection and analysis (*respond*, incident response) declined in 2023, moving these two metrics into the bottom 10.

Statistical Analysis of Function-Level Maturity as a Predictor of Overall Effectiveness

We performed a logistic regression to determine, among other things, whether function-level (*identify*, *protect*, *detect*, *respond*, and *recover*) maturity was a predictor of the overall determination of effectiveness of an agency's information security program for 2020–2022.[26] We found the following:

- From 2020 to 2022, the maturity level of the *protect* function area had a significant effect on IGs' overall determination of information security program effectiveness. On average, we found that an agency's information security program was 3.32 times more likely to be rated effective if the maturity of the *protect* function is increased by one level.
- For 2021 and 2022, we found that the maturity level of the *detect* function also had a significant effect on IGs' overall determination of information security program effectiveness. On average, we found that an agency's information security program was 3.49 times more likely to be rated effective if the maturity of the *detect* function is increased by one level.

CyberScope Survey

In addition to analyzing the IG FISMA reporting metrics, we surveyed members of the IG community on their experiences using CyberScope—the FISMA reporting application developed by DHS and used by agencies and IGs to submit their FISMA metrics. Thirty-nine OIGs responded. This survey asked questions related to IGs' overall satisfaction with the CyberScope tool, awareness of tool functionality, and desired features and capabilities in CyberScope that could improve the IG FISMA reporting process. Appendix C lists the survey questions.

Overall, the majority of survey respondents indicated that they are satisfied with the CyberScope tool and its ability to assist IGs in meeting their FISMA reporting responsibilities. However, the majority of survey respondents also indicated that they were unaware of the CyberScope training and support references available, as well as the tool's custom reporting queries and capabilities. Further, the majority of survey respondents noted that a capability within CyberScope to perform data analytics on current and prior IG submissions, as well as more robust word processing capabilities, would further assist them in meeting their FISMA reporting responsibilities.

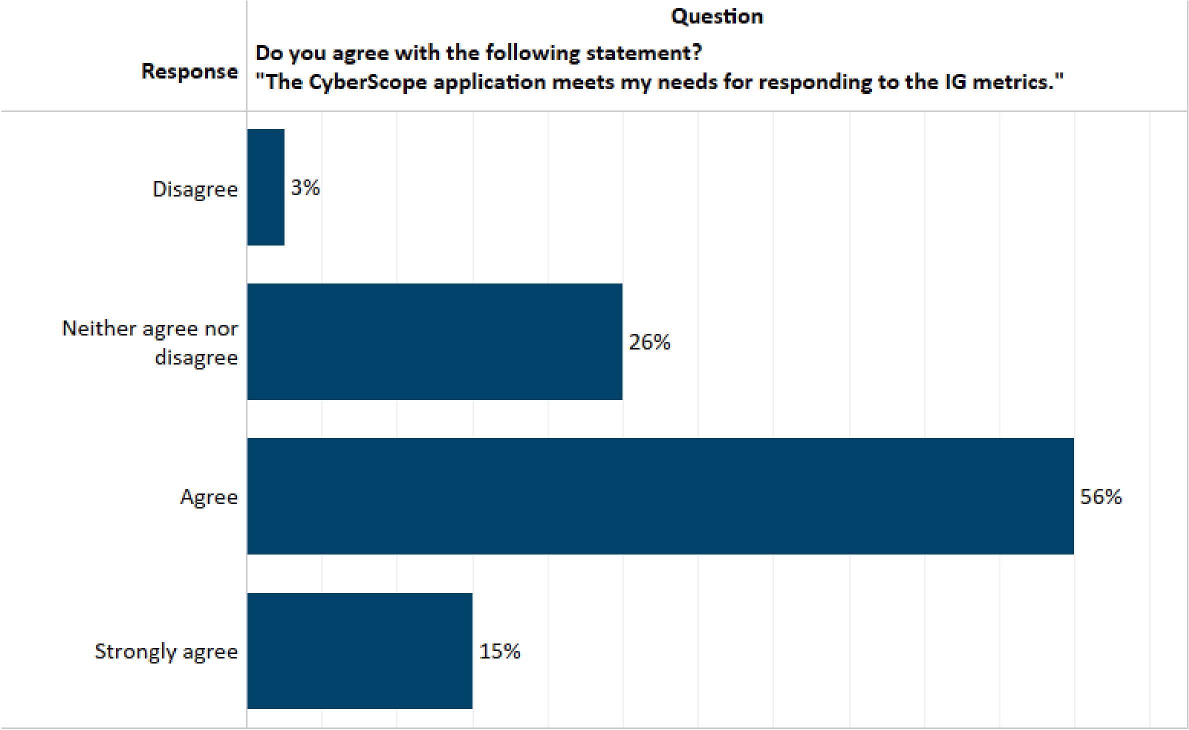
The key takeaways from the CyberScope survey are as follows:

- The majority (71 percent) of survey respondents either agreed or strongly agreed that the CyberScope application meets their needs for responding to the IG FISMA metrics (figure 15).
- The majority (56 percent) of survey respondents either agreed or strongly agreed that the CyberScope graphical user interface is easy to understand and use (figure 16).
- The majority (65 percent) of survey respondents either agreed or strongly agreed that they are satisfied with the process for obtaining/managing access to CyberScope (figure 17).

[26] Data for 2023 were not available when we performed our logistic regression.

- The majority (59 percent) of survey respondents are not familiar with CyberScope's reporting/custom queries functionality, and they would find this functionality useful (figure 18).
- The majority of survey respondents are not familiar with the CyberScope helpdesk/email function (69 percent), CyberScope training sessions/webinars (74 percent), or the CyberScope user guide (89 percent) (figure 19).
- Survey respondents ranked the following as their top five enhancements they would like to see in the CyberScope tool (figures 20 and 21):
    - improved word processing capabilities for text responses (for example, adding rich text capabilities)
    - ability to review and compare CIO FISMA metrics data against the IG FISMA metrics data[27]
    - ability to analyze their reported data from prior years
    - ability to compare IG responses governmentwide
    - ability to search current or prior year responses by term or filter (for example, maturity level, domain, or function)

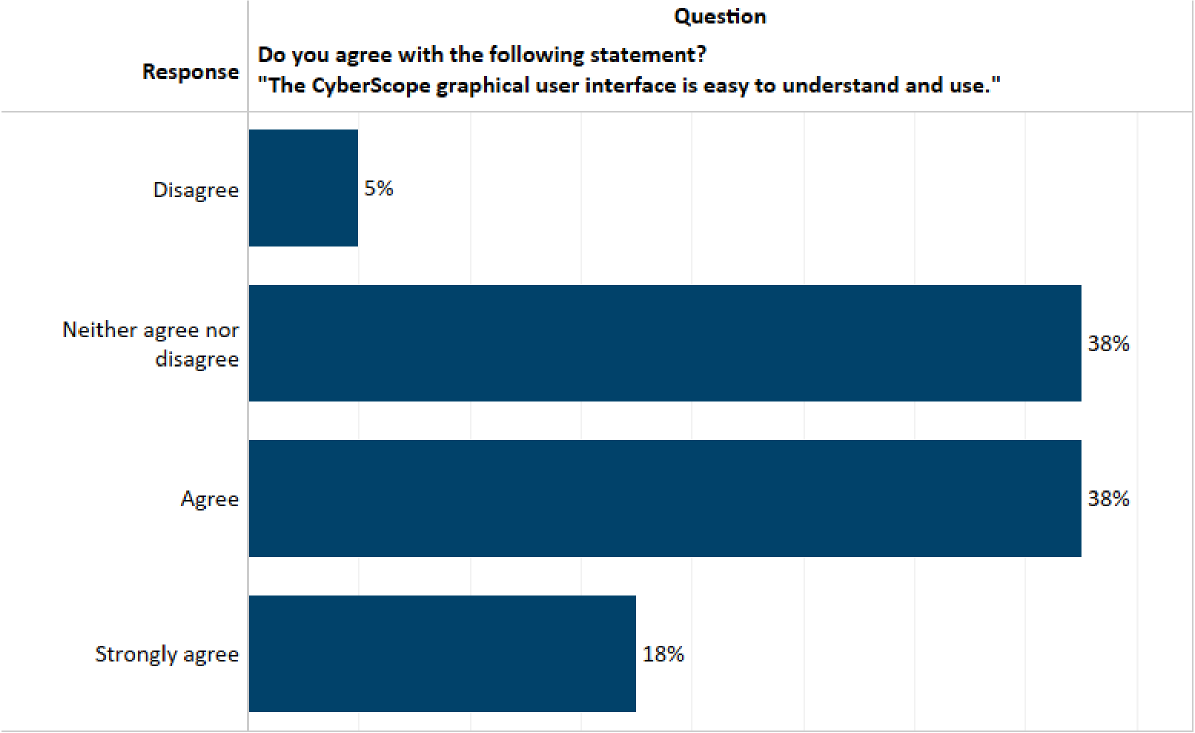
Figure 15. Satisfaction With the CyberScope Tool in Meeting IG Reporting Needs



Source: CyberScope survey responses.

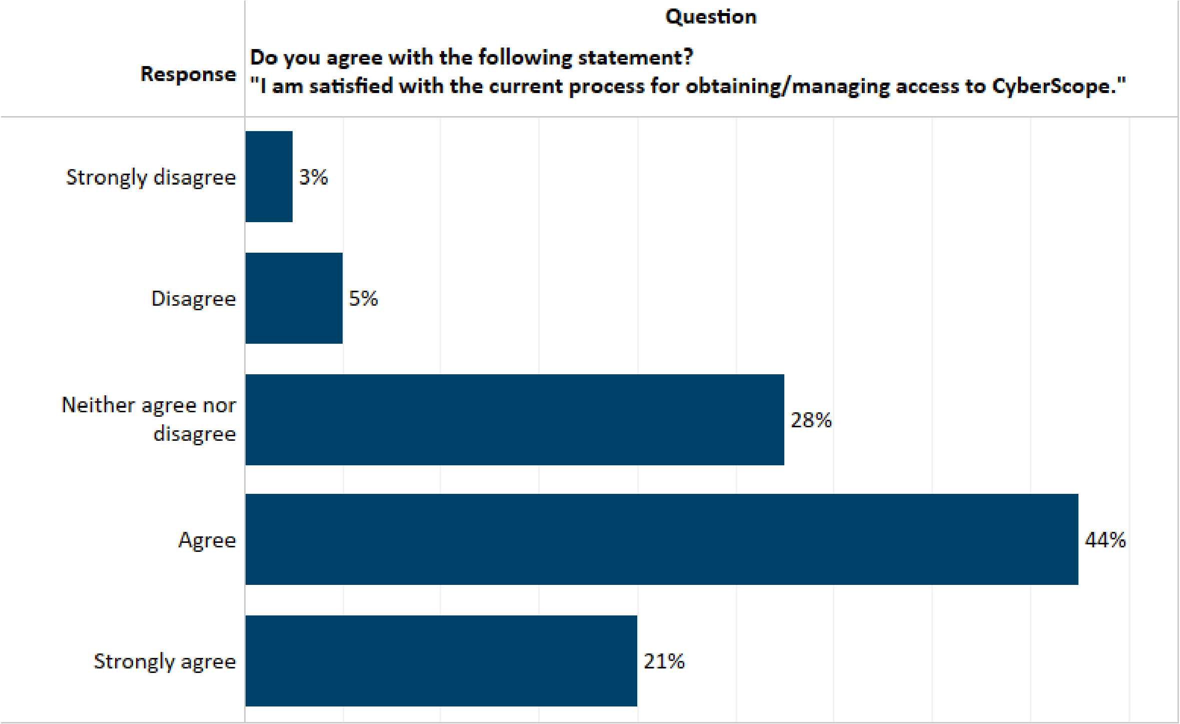
[27] Agencies report quarterly CIO metrics in the CyberScope tool as well as annual CIO metrics and metrics for the senior agency official for privacy. IGs report FISMA metrics in CyberScope annually.

Figure 16. Satisfaction With the CyberScope Graphical User Interface



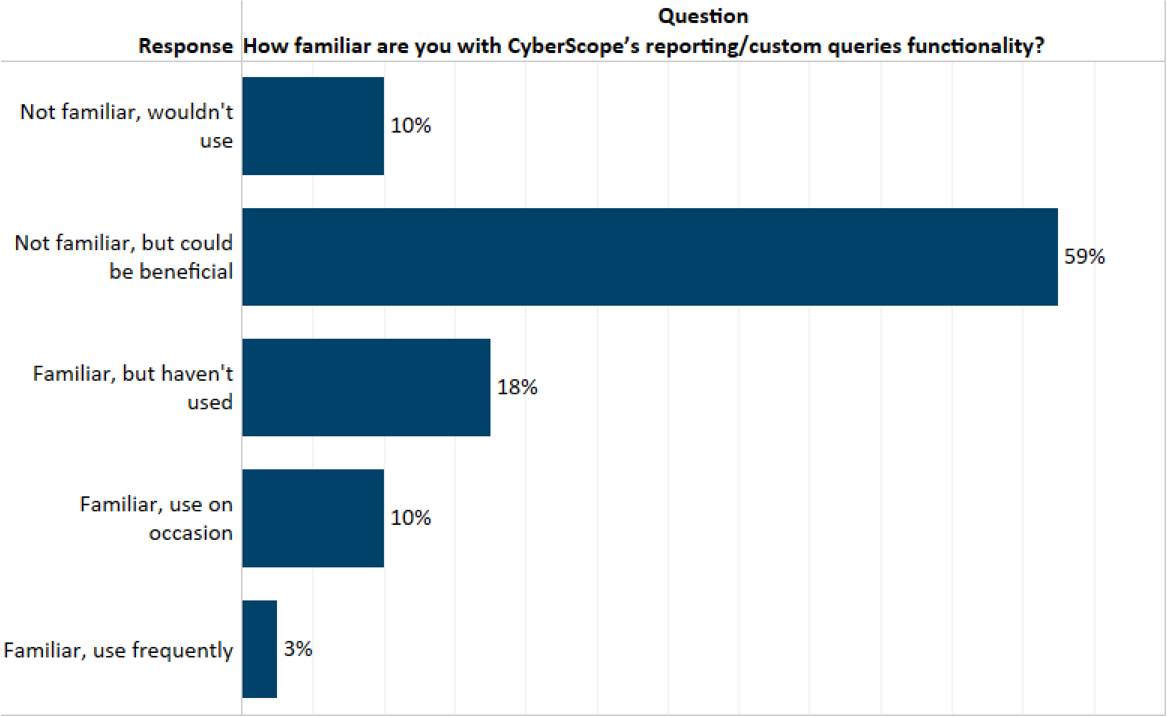
Source: CyberScope survey responses.

Figure 17. Satisfaction With Obtaining/Managing Access to CyberScope



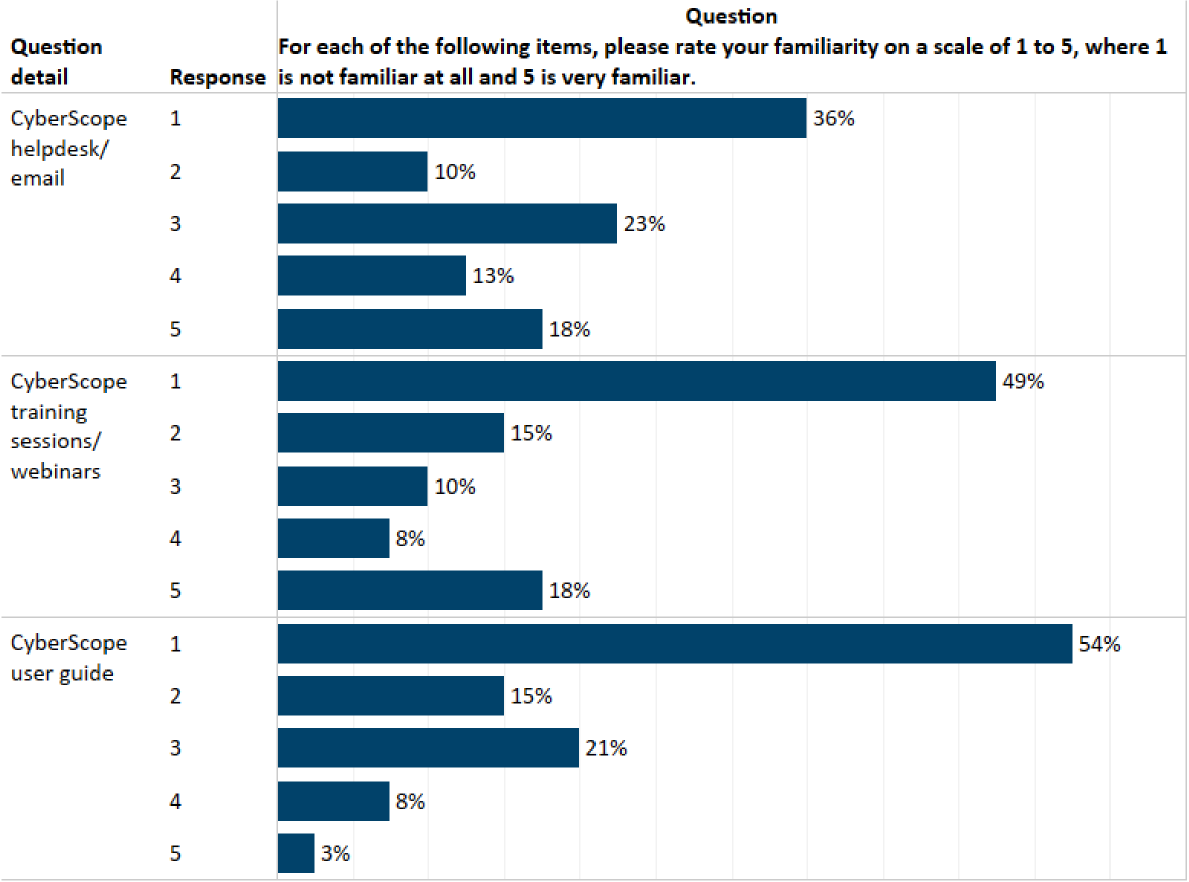
Source: CyberScope survey responses.

Figure 18. Survey Results for Awareness of CyberScope’s Reporting/Custom Queries Functionality



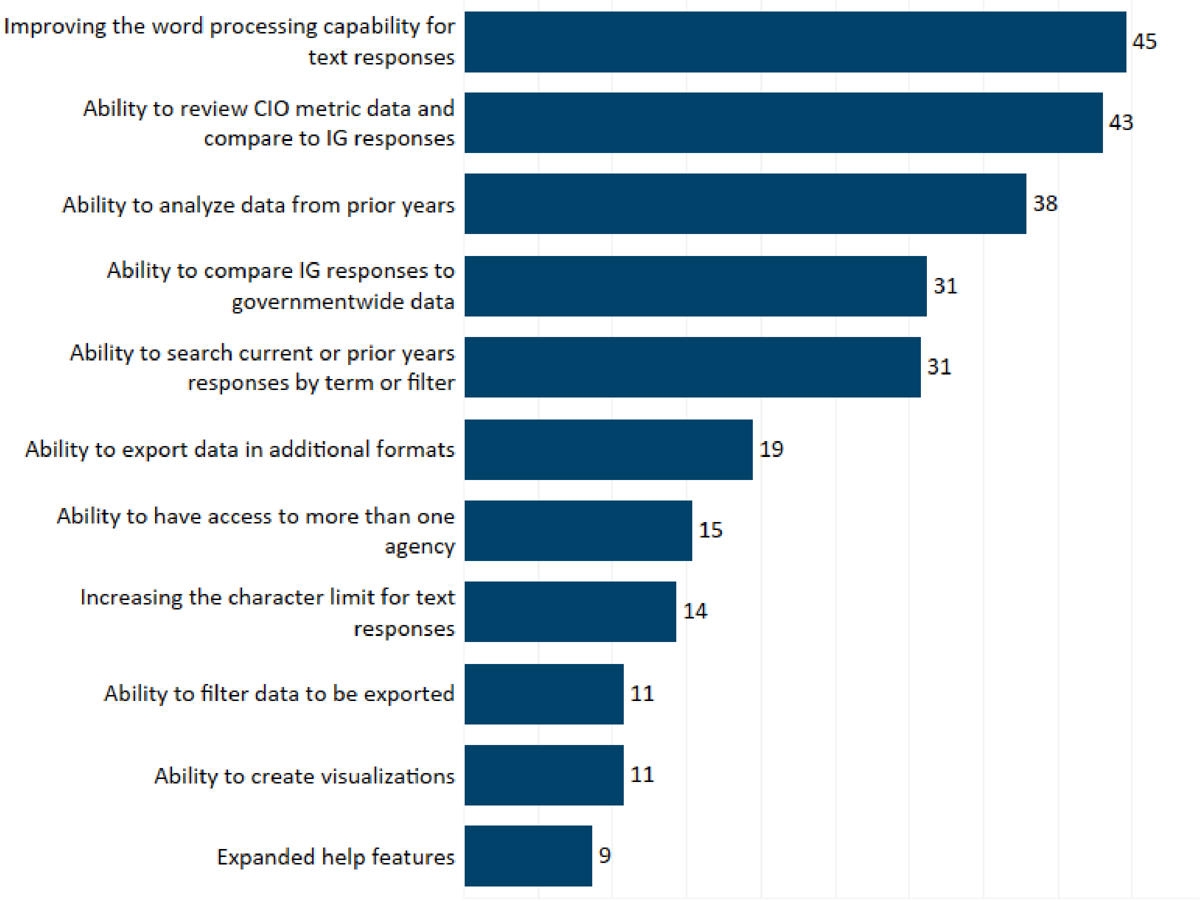
Source: CyberScope survey responses.

Figure 19. Survey Results for Familiarity With CyberScope Training and Support Resources



Source: CyberScope survey responses.

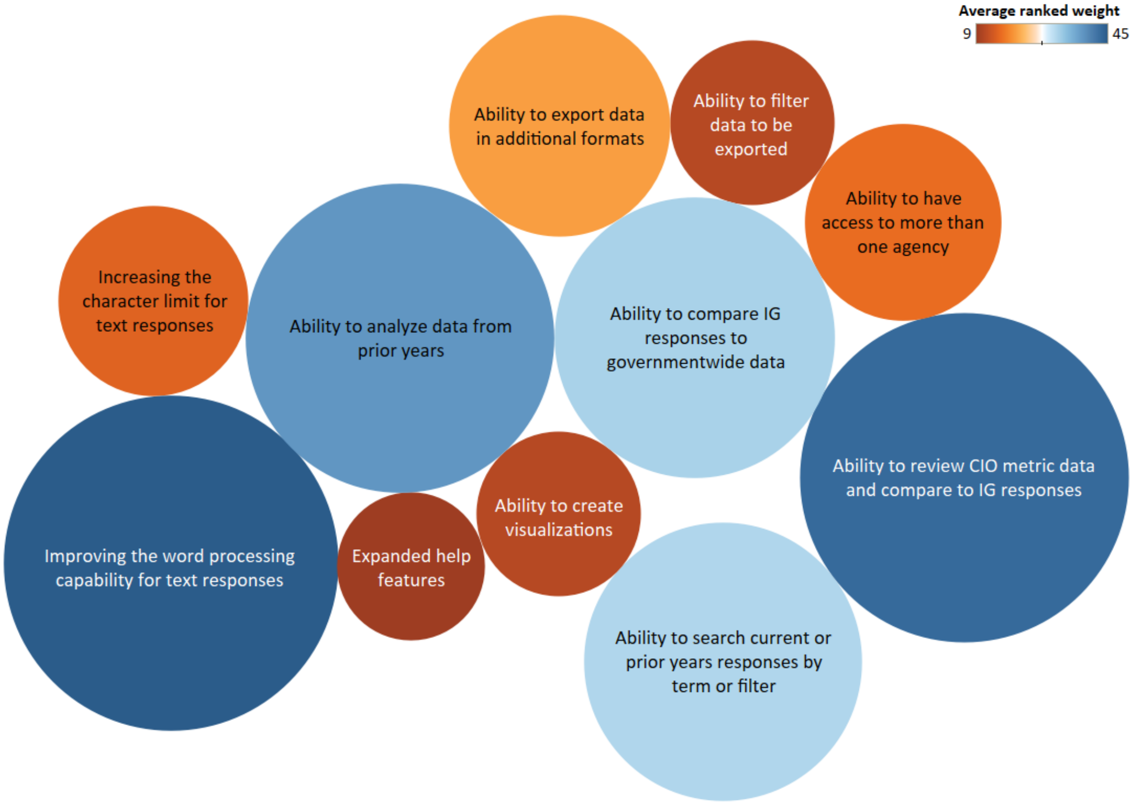
Figure 20. Survey Results for Desired Future CyberScope Capabilities



Source: CyberScope survey responses.

Note: The survey asked respondents to rank the desired future state options on a scale of 1 to 5. To develop the distribution, we assigned a weight of 1 through 5 where 1=100, 5=20, and unranked options=0. The figure represents the average rank, where 100 would be the maximum if all respondents ranked the same item as their first choice.

Figure 21. Survey Results for Desired Future CyberScope Capabilities



Source: CyberScope survey responses

Note: The survey asked respondents to rank the desired future state options on a scale of 1 to 5. To develop the distribution, we assigned a weight of 1 through 5 where 1=100, 5=20, and unranked options=0. The figure represents the average rank, where 100 would be the maximum if all respondents ranked the same item as their first choice.

Conclusion and Next Steps

Cybersecurity continues to be a key risk area for the federal government, as evidenced by cyberattacks that have targeted software supply chains, key federal systems, and critical infrastructure. These attacks are likely to continue to increase in sophistication and impact. As noted in Executive Order 14028, *Improving the Nation's Cybersecurity*, "The United States faces persistent and increasingly malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."

This project analyzed IG FISMA metrics reporting data for 2020–2023 to identify governmentwide trends in cybersecurity performance. The project also surveyed IGs on their experiences using CyberScope, the FISMA reporting application developed and maintained by DHS.

Overall, we found that federal agencies made progress to mature their information security programs during the 2020–2023 period, with the incident response and security training domains of agencies' information security programs being areas of strength. In addition, federal agencies on average have increased their maturity scores for the majority (18 of 20) of the core metrics during the 2020–2023 period. We believe that further improvements in the maturity of the core metrics will result in more agencies maintaining an effective information security program, since these metrics tie directly to administration priorities and other high-risk areas.

We found that, on average, federal agency information security programs are not as mature in the SCRM, risk management, and configuration management domains. Further, we found that while IGs are generally satisfied with CyberScope, additional functionality for data analytics and advanced word processing capabilities within the tool would assist IGs in meeting their FISMA reporting responsibilities.

The CIGIE Technology Committee plans to update this analysis periodically and use these results to continue its work with federal stakeholders on improving the IG FISMA reporting process. The committee hopes that this analysis will provide key information to stakeholders, including the American public, on the status of federal agency information security programs.

Appendix A: IG FISMA Core Metrics

Function	Domain	Core metric
Identify	Risk management	**System inventory:** To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?
Identify	Risk management	**Hardware asset management:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including government-furnished equipment and Bring Your Own Device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
Identify	Risk management	**Software asset management:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
Identify	Risk management	**Information security risk management:** To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?
Identify	Risk management	**Cyber risk reporting:** To what extent does the organization utilize technology/automation to provide a centralized, enterprisewide (portfolio) view of CSRM activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
Identify	SCRM	**Third-party security:** To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
Protect	Configuration management	**Configuration settings:** To what extent does the organization utilize settings/common secure configurations for its information systems?

Function	Domain	Core metric
Protect	Configuration management	**Flaw remediation:** To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?
Protect	Identity and access management	**Multifactor authentication (nonprivileged users):** To what extent has the organization implemented strong authentication mechanisms (personal identity verification [PIV] or an identity assurance level [IAL]3/authenticator assurance level [AAL]3 credential) for nonprivileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Protect	Identity and access management	**Multifactor authentication (privileged users):** To what extent has the organization implemented strong authentication mechanisms (PIV or an IAL3/AAL3 credential) for privileged users to access the organization's facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Protect	Identity and access management	**Privileged account management:** To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?
Protect	Data protection and privacy	**Privacy controls:** To what extent has the organization encrypted data at rest and in transit, limited the transference of data by removable media, and sanitized digital media before disposal or reuse to protect its personal identifiable information and other agency sensitive data, as appropriate, throughout the data life cycle?
Protect	Data protection and privacy	**Enhanced network protections:** To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?
Protect	Security training	**Cyber workforce assessment:** To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the function areas of *identify*, *protect*, *detect*, *respond*, and *recover*?

Function	Domain	Core metric
Detect	ISCM	**ISCM strategy, policies, and procedures:** To what extent does the organization utilize ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
Detect	ISCM	**Ongoing assessments and authorizations:** How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations (including developing and maintaining system security plans), and monitoring system security controls?
Respond	Incident response	**Incident detection and analysis:** How mature are the organization's processes for incident detection and analysis?
Respond	Incident response	**Incident handling:** How mature are the organization's processes for incident handling?
Recover	Contingency planning	**Business impact analysis:** To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?
Recover	Contingency planning	**Contingency plan testing:** To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Source: OIG analysis of Office of Management and Budget, Office of the Federal Chief Information Officer, *FY22 Core IG Metrics Implementation Analysis and Guidelines*, January 2022.

Appendix B: Distribution of IG FISMA Core Metrics, 2022–2024

CSF function	Domain	Number of core metrics	Number of supplemental metrics
Identify	Risk management	5	5
	SCRM	1	3
Protect	Configuration management	2	6
	Identity and access management	3	5
	Data protection and privacy	2	3
	Security training	1	4
Detect	ISCM	2	2
Respond	Incident response	2	5
Recover	Contingency planning	2	4
Total		20	37

Appendix C: IG CyberScope Survey Questions

Question	Answer choices (if applicable)
Agency Background	
1. What is the name of your agency?	
2. Please select your agency type.	(a) Small/independent (b) CFO Act (c) Other
3. How many individuals in your OIG have access to CyberScope?	
4. What roles do individuals with CyberScope access have in your OIG (select all that apply)?	(a) Executive Management (ex. IG, Deputy IG, AIG) (b) Management (ex. Audit Managers) (c) Staff (ex. Auditors, Analysts)
Respondent Background	
5. What role most closely matches your agency title?	(a) Executive Management (ex. IG, Deputy IG, AIG) (b) Management (ex. Audit Managers) (c) Staff (ex. Auditors, Analysts)
6. What is your role in CyberScope (select all that apply)	(a) FISMA IG Data Entry/Validate (b) FISMA IG Submitter
7. How many years have you used CyberScope?	(a) Less than 1 year (b) 1–3 years (c) More than 3 years

Question	Answer choices (if applicable)
CyberScope Functionality: Current State	
8. Do you agree with the following statement: “I am satisfied with the current process for obtaining/managing access to CyberScope”?	(a) Strongly disagree (b) Disagree (c) Neither agree nor disagree (d) Strongly agree
9. How familiar are you with CyberScope’s Reporting/Custom Queries functionality?	(a) Not familiar, wouldn’t use (b) Not familiar, but could be beneficial (c) Familiar but haven’t used (d) Familiar, use on occasion (e) Familiar, use frequently
10. Do you agree with the following statement? “The CyberScope graphical user interface is easy to understand and use.”	(a) Strongly disagree (b) Disagree (c) Neither agree nor disagree (d) Strongly agree
11. Do you agree with the following statement? “The CyberScope application meets my needs for responding to the IG metrics.”	(a) Strongly disagree (b) Disagree (c) Neither agree nor disagree (d) Strongly agree
12. For each of the following items, please rate your familiarity on a scale of 1 to 5, where 1 is not familiar at all and 5 is very familiar.	(a) CyberScope Helpdesk/email (b) CyberScope User Guide (c) CyberScope Training Sessions/Webinar
13. Please provide comments, if desired, to help us understand the above rating (#12).	
14. For each of the following items, please rate its usefulness on a scale of 1 to 5, where 1 is not useful at all and 5 is very useful.	(a) CyberScope Helpdesk/email (b) CyberScope User Guide (c) CyberScope Training Sessions/Webinar
15. Please provide comments, if desired, to help us understand the above rating (#14).	

Question	Answer choices (if applicable)
CyberScope Functionality: Future	
16. What features would you like to see added or improved in CyberScope? (Please rank your top 5 selections.)	(a) Increasing the character limit for text responses (b) Improving the word processing capability for text responses (i.e., maintaining formatting when using copy/paste, ability to format text, etc.) (c) Ability to have access to more than one agency (d) Ability to analyze data from prior years (e) Ability to review CIO metric data and compare to IG responses (f) Ability to search current or prior years responses by term or filter (maturity level, domain, function, etc.) (g) Ability to compare IG responses to governmentwide data (h) Ability to create visualizations (i) Ability to export data in additional formats (Word, Excel, etc.) (j) Ability to filter data to be exported (i.e., core vs. supplemental metrics) (k) Expanded help features (such as FAQs, knowledgebase etc.)
17. Other features (please specify)	
18. What kind of training options would you like to see in the future? (Select as many as apply.)	(a) Live in-person (b) Virtual (c) On-demand/self-paced (d) User Guide/FAQs
19. Please provide comments, if desired, on training topics you would like to see and recommended frequency of training.	
20. Please provide any additional feedback on the CyberScope application.	

Abbreviations

AAL	authenticator assurance level
CFO Act	Chief Financial Officers Act of 1990
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
CSF	Cybersecurity Framework
CSRM	cybersecurity risk management
DHS	U.S. Department of Homeland Security
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	U.S. Government Accountability Office
HVA	high-value asset
IAL	identity assurance level
IG	inspector general
ISCM	information security continuous monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	personal identity verification
SCRM	supply chain risk management

Report Contributors

Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau OIG
National Science Foundation OIG
U.S. Department of Commerce OIG
U.S. Department of Defense OIG
U.S. Department of Homeland Security OIG
U.S. Securities and Exchange Commission OIG