TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation

August 2, 2023

Report Number: 2023-20-041

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation

Final Audit Report issued on August 2, 2023 | **Report Number 2023-20-041**

Why TIGTA Did This Audit

As part of the Federal Information Security Modernization Act of 2014 (FISMA) legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices.

Our overall objective was to assess the effectiveness of the IRS's information security program on a maturity model spectrum based on the *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics*.

Impact on Tax Administration

FISMA focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. In Fiscal Year 2022, the IRS received and processed more than 262.8 million Federal tax returns and supplemental documents, which represents a substantial amount of taxpayer personal and financial information. As the custodian of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss.

The IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA requirements; otherwise, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

What TIGTA Found

The IRS Cybersecurity Program was not considered fully effective due to program components that were not at an acceptable maturity level. The *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics* scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

TIGTA reviewed the FISMA reporting metrics for Fiscal Year 2023 and found:

The IRS Cybersecurity Program was considered not fully effective.

TIGTA rated three Cybersecurity Framework function areas as "not-effective" and two as "effective." The IDENTIFY, PROTECT, and DETECT capabilities are "not effective" and the RESPOND and RECOVER capabilities are "effective" based on a *Managed and Measurable* – Level 4 rating.

As examples of specific metrics that were not considered effective, TIGTA found that the IRS could improve on maintaining a comprehensive and accurate inventory of its information systems; tracking and reporting on an up-to-date inventory of hardware and software assets; ensuring that its information systems consistently maintain baseline configuration in compliance with IRS policy; implementing flaw remediation and patching on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its facilities and network.

For Fiscal Year 2023, the Inspector General FISMA reporting was aligned with the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and measured the maturity level for five function areas. The five Cybersecurity Framework function areas and the associated security program component(s) are IDENTIFY (Risk Management and Supply Chain Risk Management), PROTECT (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), DETECT (Information Security Continuous Monitoring), RESPOND (Incident Response), and RECOVER (Contingency Planning).

What TIGTA Recommended

TIGTA does not make recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines for the applicable FISMA evaluation period. The IRS provided a response to a draft of this report and disagreed with our assessment regarding their Event Logging maturity rating. TIGTA's analysis of this response is included in an appendix to this report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

August 2, 2023

MEMORANDUM FOR: ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation (Audit # 202320001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act of 2014 evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2023.[1] The Act requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. Our overall objective was to assess the effectiveness of the IRS's information security program on a maturity model spectrum based on the *Fiscal Years 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. This audit is included in our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources.*

This report is being forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury's Chief Information Officer.

Management's complete response to the draft report is included as Appendix III. If you have questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] 44 U.S.C. § 3551, et seq. (2018).

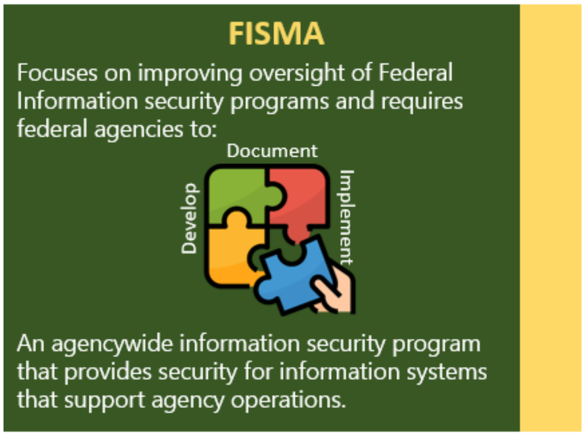
Table of Contents

Appendices

Background

The Federal Information Security Modernization Act of 2014, hereafter referred to as FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses.[1]

It requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. It assigns specific responsibilities to agency heads and Inspectors General in complying with the requirements of FISMA and is supported by the Office of Management and Budget (OMB), the Department of Homeland Security, agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.



FISMA

Focuses on improving oversight of Federal Information security programs and requires federal agencies to:

An agencywide information security program that provides security for information systems that support agency operations.

For example, FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the OMB. These independent evaluations are to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. FISMA oversight for the Department of the Treasury is performed by the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of Inspector General. TIGTA is responsible for oversight of the Internal Revenue Service (IRS) while the Treasury Office of Inspector General is responsible for all other Treasury Department bureaus. The Treasury Office of Inspector General has overall responsibility to combine the results for all the bureaus into one report for the OMB.

Overview of the IRS

The IRS's mission is to provide taxpayers with top quality service by helping them understand and meet their tax responsibilities and enforcing the law with integrity and fairness to all. In Fiscal Year 2022, the IRS collected more than $4.9 trillion in gross taxes and processed more than 262.8 million Federal tax returns and supplemental documents, which represents a substantial amount of taxpayer personal and financial information. As the custodian of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss.

[1] 44 U.S.C. § 3551, et seq. (2018).

Within the IRS, the Information Technology organization's Cybersecurity function is responsible for protecting taxpayer information and the electronic systems, services, and data from internal and external cybersecurity-related threats by implementing security practices in planning, implementation, management, and operations. The Cybersecurity function is tasked with preserving the confidentiality, integrity, and availability of IRS systems and its data.

Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics Requirements

The *Fiscal Years 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 10, 2023) was developed as a collaborative effort amongst the OMB and the Council of the Inspectors General on Integrity and Efficiency, with review and feedback provided by several stakeholders, including the Federal Chief Information Officer and Chief Information Security Officer councils.

In Fiscal Year 2022, the OMB and the Council of the Inspectors General on Integrity and Efficiency shifted the evaluation process to a two-year cycle with a set of core metrics that must be evaluated annually. These 20 core reporting metrics are a subset of the 66 reporting metrics from the Inspector General FISMA Reporting Metrics and represent a combination of administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness. Specifically, these core metrics align with the Executive Order on Improving the Nation's Cybersecurity and guidance from the OMB to agencies to improve Federal cybersecurity.[2]

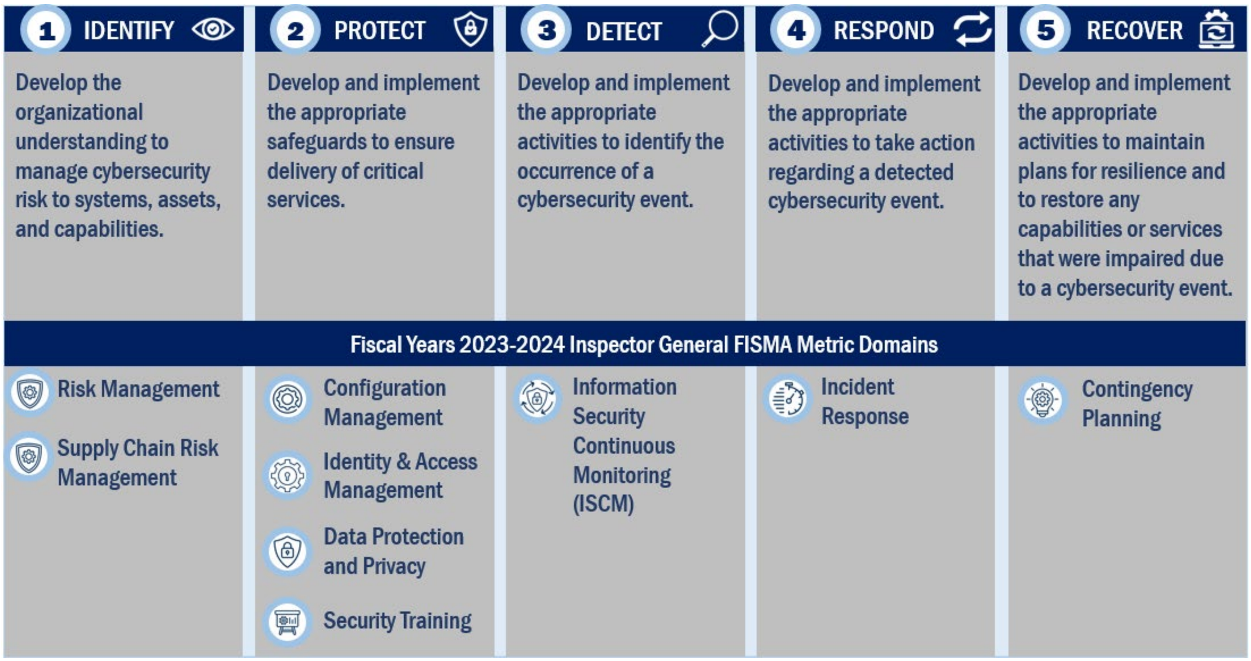
For Fiscal Year 2023, the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics* represents a continuation of the work that began in Fiscal Year 2022, with a set of 20 core metrics that must be evaluated annually and the addition of 20 supplemental metrics. The supplemental metrics are assessed at least every two years and represent important activities conducted by security programs, and contribute to the overall evaluation and determination of security program effectiveness.

The *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics* aligns with the five cybersecurity function areas in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, hereafter referred to as the Cybersecurity Framework.[3] Figure 1 presents the five Cybersecurity Framework function areas and aligns each with the associated security program component(s) (or metric domain(s)).

[2] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021); OMB, Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 27, 2021); OMB, Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (Oct. 8, 2021); OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022); and OMB, Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022).

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 2018).

Figure 1: Alignment of NIST Cybersecurity Framework Function Areas to the Fiscal Years 2023-2024 Inspector General FISMA Metric Domains

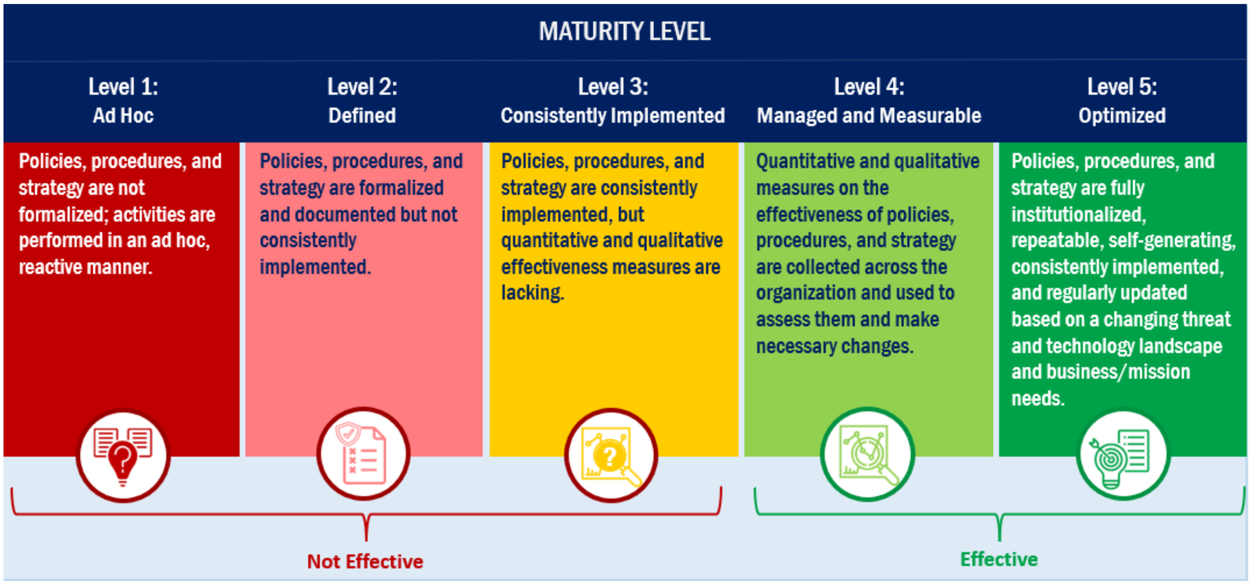


1 IDENTIFY	2 PROTECT	3 DETECT	4 RESPOND	5 RECOVER
Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Fiscal Years 2023-2024 Inspector General FISMA Metric Domains				
Risk Management Supply Chain Risk Management	Configuration Management Identity & Access Management Data Protection and Privacy Security Training	Information Security Continuous Monitoring (ISCM)	Incident Response	Contingency Planning

Source: Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics and NIST Framework for Improving Critical Infrastructure Cybersecurity.

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institute those policies and procedures. Maturity levels range from *Ad Hoc* for not having formalized policies, procedures, and strategies to *Optimized* for fully institutionalizing sound policies, procedures, and strategies across the agency. Figure 2 details the five maturity levels: *Ad Hoc, Defined, Consistently Implemented, Managed and Measurable*, and *Optimized*. The scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

Figure 2: Inspector General's Assessment Maturity Levels



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

Source: Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics.

The Inspectors General will assess the overall maturity of the agency's information security program using the average rating of the individual function areas (IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER), with the core and supplemental ratings averaged independently.

The OMB strongly encourages Inspectors General to focus on the results of the core metrics, as these tie directly to administration priorities and other high-risk areas. Per the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, the Inspectors General should use the calculated averages of the supplemental metrics to support their risk-based determination of overall program and function level effectiveness.

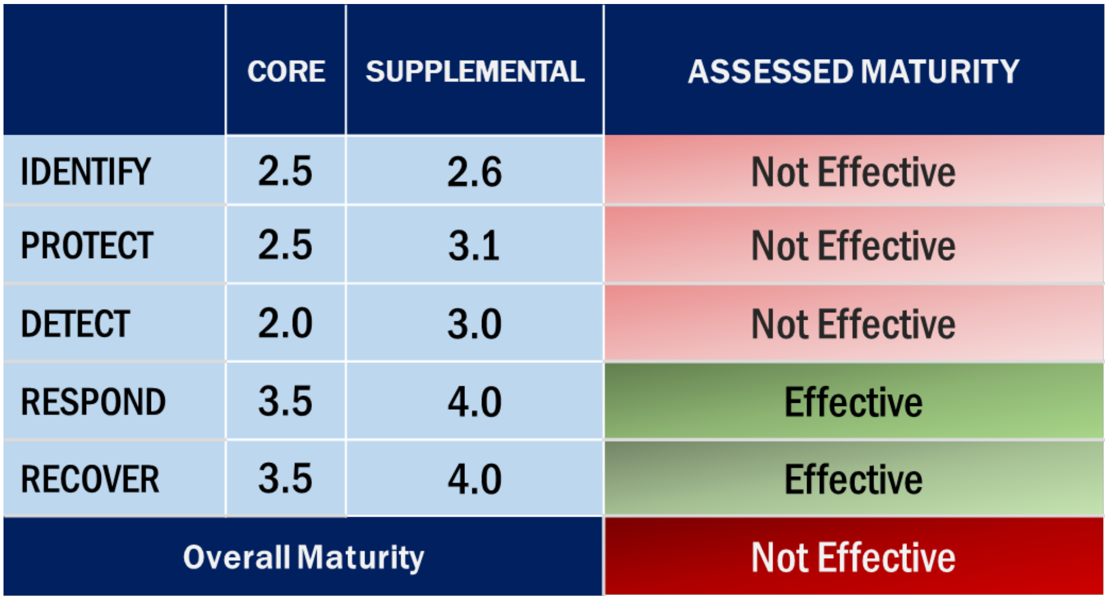
The Inspectors General may consider the results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing; the progress made by agencies to address outstanding Inspector General recommendations; and reported security incidents during the review period.

Results of Review

The IRS Cybersecurity Program Was Not Effective in Three of the Five Cybersecurity Function Areas

The IRS's Cybersecurity Program was generally aligned with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. However, due to program components that were not at an acceptable maturity level, the Cybersecurity Program was not considered fully effective. As shown in Figure 3, TIGTA rated three Cybersecurity Framework function areas as "not-effective" and two as "effective." The IDENTIFY, PROTECT, and DETECT capabilities are not effective and the RESPOND and RECOVER capabilities are effective. In determining the overall effectiveness of the IRS's information security program, as instructed by the *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics*, TIGTA focused on the results of the core metrics and used the supplemental metrics to support the overall function level effectiveness. In addition, TIGTA has the discretion to determine that an IRS's information program is effective even if it does not achieve a Level 4, *Managed and Measurable*. Figure 3 presents the Cybersecurity Framework function areas ratings averaged independently to determine a function's assessed maturity.

Figure 3: Fiscal Year 2023 Inspector General Cybersecurity Framework Assessment Results



	CORE	SUPPLEMENTAL	ASSESSED MATURITY
IDENTIFY	2.5	2.6	Not Effective
PROTECT	2.5	3.1	Not Effective
DETECT	2.0	3.0	Not Effective
RESPOND	3.5	4.0	Effective
RECOVER	3.5	4.0	Effective
Overall Maturity			Not Effective

Source: TIGTA's evaluation of security program metrics that determined whether Cybersecurity Framework function areas were rated "effective" or "not effective."

As examples of specific metrics that were not considered effective, TIGTA found that the IRS could improve on maintaining a comprehensive and accurate inventory of its information systems; tracking and reporting on an up-to-date inventory of hardware and software assets, ensuring that its information systems consistently maintain baseline configuration in compliance with IRS policy; implementing flaw remediation and patching on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its facilities and network. Details of the results of our evaluation of IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER are presented on pages 6, 11, 18, 20, and 22, respectively.

The IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA requirements; otherwise, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

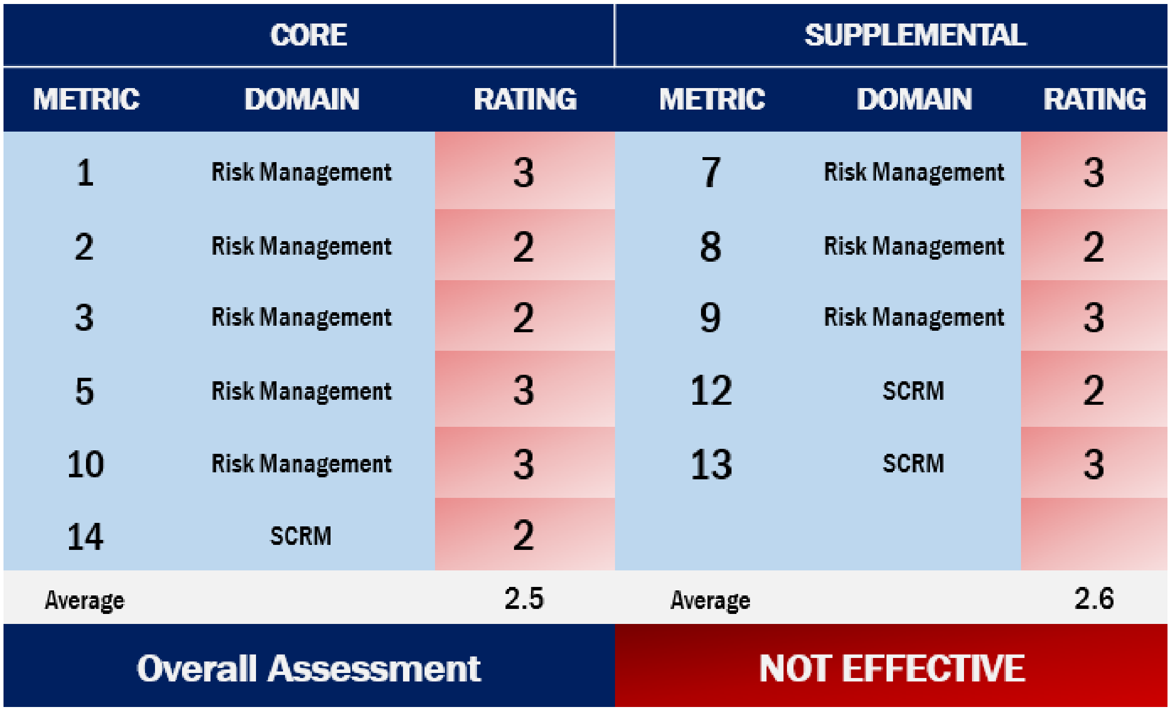
To determine the effectiveness of the Cybersecurity Program, we evaluated the maturity level of the program metrics specified by the Department of Homeland Security in the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*. Along with our review of pertinent documents and discussions with IRS subject matter experts, we based our evaluation on a representative subset of seven information systems and the implementation status of key security controls as well as considered the results of TIGTA and Government Accountability Office (GAO) audits. These audits, whose results were applicable to FISMA metrics, were performed, completed, or contained recommendations that were still open during the FISMA evaluation period, July 1, 2022, to June 2, 2023. See Appendix II for a list of these audits with notations as to which metric(s) the reports applied.

The detailed results of our evaluation of the maturity level for each of the Fiscal Year 2023 Inspector General Metrics are provided below. The metrics are based on Federal Government guidance and criteria, such as NIST, Special Publication 800-53, Revision 5; Executive Order 14028; and OMB memoranda.[4] For metrics rated lower than a maturity level 4, *Managed and Measurable*, we have provided comments to explain our determinations. The effectiveness rating for core metrics and supplemental metrics averages were calculated independently based on the Cybersecurity Framework function areas. However, we also considered other factors to determine the final ratings, as instructed by the *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics.*

The Cybersecurity Framework function area of IDENTIFY was rated as Not Effective

Based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, we found that the IDENTIFY function area and the respective domains, Risk Management and Supply Chain Risk Management (SCRM), met a Core maturity level of 2.5 and a Supplemental maturity level of 2.6, which we considered "not effective." Figure 4 presents the maturity level ratings for the assessed metrics.

Figure 4: Fiscal Year 2023 IDENTIFY Function Area Assessment Results



CORE			SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
1	Risk Management	3	7	Risk Management	3
2	Risk Management	2	8	Risk Management	2
3	Risk Management	2	9	Risk Management	3
5	Risk Management	3	12	SCRM	2
10	Risk Management	3	13	SCRM	3
14	SCRM	2			
Average		2.5	Average		2.6
Overall Assessment			NOT EFFECTIVE		

[4] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020); Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021); OMB, Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures* (Aug. 10, 2021); OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022); OMB, Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices* (Sept. 14, 2022); and OMB, Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 2, 2022).

Source: TIGTA's evaluation of security program metrics associated with the Cybersecurity Framework function area IDENTIFY.

IDENTIFY Function Area – Risk Management

1. 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?

   Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently implements its policies, procedures, and processes to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.

   Comments: While the IRS provided a list of inventories of information systems and system interconnections, it cannot ensure that information systems included in its inventory are accurate and complete as the IRS Information Security Continuous Monitoring (ISCM) Program Plan indicates gaps in tools used to monitor its system inventories. In addition, the IRS is seeking further confirmation with the third party to determine whether Interconnections System Agreements are required and renewing expired Interconnections System Agreements.

2. 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?[5]

   Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.

   Comments: While the IRS has policies and procedures to maintain an up-to-date inventory of hardware assets, it has not closed scanning tool gaps necessary to perform checks for unauthorized hardware components/devices and to notify appropriate organizational officials. The IRS has open Plan of Action and Milestones (POA&M) related to failure to maintain an accurate system inventory and components. However, the IRS can identify hardware assets by category reported to the Department of the Treasury. In addition, the IRS is in the process of performing data quality reviews to ensure the accuracy and quality of the data.

3. 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?

   Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for

[5] Taxonomy is a scheme of classifications.

Executive Order-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.

Comments: While the IRS has policies for maintaining an up-to-date inventory of software assets, it does not have a tool that can detect the presence of unauthorized software and notify appropriate organizational officials. According to the IRS, it is in the process of deploying a software asset management tool for conducting passive scanning. Further, the IRS plans to assess controls related to critical software.

5. 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?

   Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.

   Comments: The IRS uses a cybersecurity risk register to manage risks; however, the documentation to support risk snapshots for six (86 percent) of the seven sample information systems were initially reported as either not available or not adequate. Subsequently, the IRS indicated that there are processes in place to support the risk management process and strategy. Further, the IRS is expanding system risk snapshots to non-filing season applications with a targeted completion date of September 2023.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?

   Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – Individuals are consistently performing the cybersecurity risk management roles and responsibilities that have been defined across the organization. This includes roles and responsibilities related to integration with enterprise risk management processes, as appropriate.

   Comments: While the IRS met consistently implemented, the evidence provided by the IRS was not sufficient. The IRS provided the risk register, which captures the top risks strategic, operations, reporting, and compliance category; however, it is missing the enterprise-wide risk overview. In addition, the IRS performance dashboards designed to monitor progress do not capture completed cybersecurity risk management activities.

8. To what extent has the organization ensured that POA&Ms are used for effectively mitigating security weaknesses?

   Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, monitoring and maintenance, and independent validation of POA&M activities.

   Comments: The IRS has not consistently implemented POA&M policies and procedures to effectively manage security weaknesses. Our review of the POA&Ms, as of March 9, 2023, showed that the IRS had 1,258 active POA&Ms. We found that 598 (48 percent) of the 1,258 active POA&Ms were classified as late. Also, we found that 552 (92 percent) of the 598 active POA&Ms classified as late had a risk severity rating of moderate or higher. Specifically, we found one critical, 37 high, and 514 moderate risk severity POA&Ms. The IRS did not include the risk severity on two of the 598 active POA&Ms. The 598 active POA&Ms classified as late have been open from 85 to 3,899 days. In addition, the IRS has open recommendations in prior TIGTA reports for not creating and completing POA&Ms timely based on IRS-defined timelines and processes.

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?

   Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently uses a cybersecurity risk register, or other comparable mechanism, to ensure that information about risks is communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed. Further, processes to share cybersecurity risk information are integrated with the organization's ISCM processes.

   Comments: The IRS uses a cybersecurity risk register to ensure that information about risks is communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know. As reported last year, TIGTA continues to identify System Security Plans that did not always meet quality standards. For example, we found System Security Plans with privacy controls that were not classified correctly and captured all fields in the security assessment and monitoring system. Without quality information, management's (including internal and external stakeholders) ability to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks is limited.

10. To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.

Comments: The *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics* lists OMB Memorandum M-22-09, as criteria for this metric.[6] The memorandum sets forth a Federal Zero Trust Architecture strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. According to the IRS, it is tracking the status of the planned items presented in the Zero Trust Strategy Implementation Plan. While the full Zero Trust Architecture implementation is not required until Fiscal Year 2024, TIGTA reported that the IRS has completed several activities including developing a reference architecture plan and roadmap.

IDENTIFY Function Area – Supply Chain Risk Management

12. To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined and communicated an organization-wide SCRM strategy. The strategy addresses SCRM risk appetite and tolerance, SCRM strategies or controls, processes for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the SCRM strategy, and associated roles and responsibilities.

    Comments: The IRS SCRM Program Strategy is led by the Cybersecurity SCRM program office, and the strategy has been communicated organization wide. The Cybersecurity SCRM program office will manage all activities for information and communication technologies and service across the entire IRS. According to the IRS, the Cybersecurity Supply Chain Risk Assessments Pilot Program is preparing the IRS for its full deployment of the Cybersecurity SCRM Program. The IRS has transitioned to full program deployment and has initiated the data collection phase for the next assessments.

13. To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently implements its policies, procedures, and processes for managing supply chain risks for [organizationally-defined] products, systems, and services provided by third parties. Further, the organization uses lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined time frame.

    Comments: According to the IRS, it had a successful execution of the Cybersecurity Supply Chain Risk Assessment Pilot and has policies and procedures to consistently implement the Cybersecurity SCRM Program.

[6] OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).

14. 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?

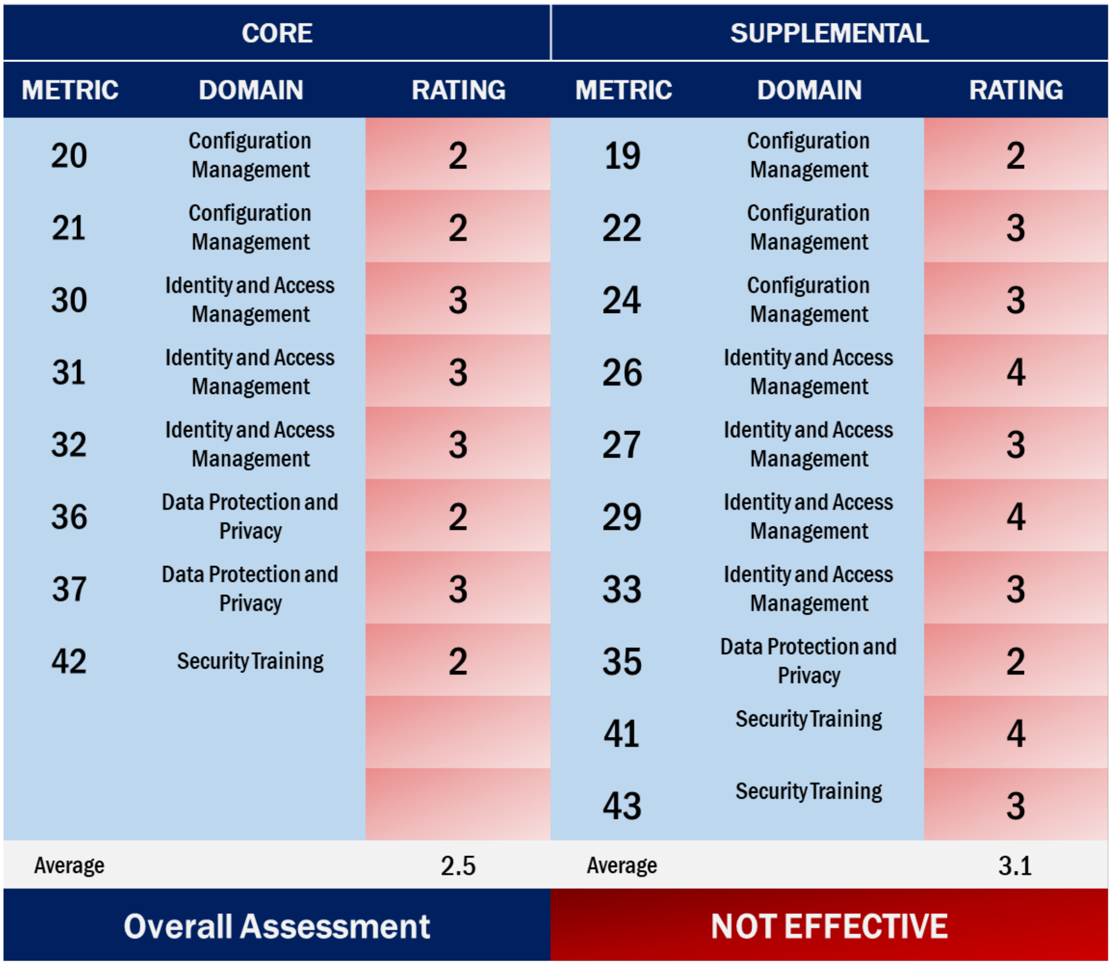
    Maturity Level and Corresponding Narrative: *Defined (Level 2)* – The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.

    Comments: While the IRS has defined and communicated policies and procedures, it has not fully implemented its cybersecurity supply chain risk assessment process that includes assessing and reviewing the supply chain-related risks associated with suppliers or contractors and system components.

The Cybersecurity Framework function area of PROTECT was rated as Not Effective

Based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, we found that the PROTECT function area and the respective domains, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training, met a Core maturity level of 2.5 and a Supplemental maturity level of 3.1, which we considered "not effective." Figure 5 presents the maturity level ratings for the assessed metrics.

Figure 5: Fiscal Year 2023 PROTECT Function Area Assessment Results



CORE			SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
20	Configuration Management	2	19	Configuration Management	2
21	Configuration Management	2	22	Configuration Management	3
30	Identity and Access Management	3	24	Configuration Management	3
31	Identity and Access Management	3	26	Identity and Access Management	4
32	Identity and Access Management	3	27	Identity and Access Management	3
36	Data Protection and Privacy	2	29	Identity and Access Management	4
37	Data Protection and Privacy	3	33	Identity and Access Management	3
42	Security Training	2	35	Data Protection and Privacy	2
			41	Security Training	4
			43	Security Training	3
Average		2.5	Average		3.1
Overall Assessment			NOT EFFECTIVE		

Source: TIGTA's evaluation of security program metrics associated with the Cybersecurity Framework function area PROTECT.

PROTECT Function Area – Configuration Management

19. To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.

    Comments: The IRS has not fully defined baseline configurations for its information systems and has not consistently maintained its inventory of related components. In addition, the IRS has several open POA&Ms documenting its weaknesses in maintaining configuration baselines.

20. To what extent does the organization use configuration settings/common secure configurations for its information systems?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.

    Comments: While the IRS has policies and procedures for configuration settings, it has not consistently implemented secure configuration settings for its information systems. The IRS has open POA&Ms documenting system weaknesses due to deficiencies in configuration setting, software authorization, least functionality, and vulnerability monitoring and scanning. In addition, the GAO reported that deficiencies exist concerning improper configuration of security settings.

21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable internet protocol assets?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational-defined time frames, and incorporating flaw remediation into the organization's configuration management processes.

    Comments: While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis. Several TIGTA reports found the IRS did not remediate vulnerabilities or install security patches on systems in a timely manner. In addition, the IRS has open POA&Ms that document weaknesses in flaw remediation and malicious code protection. Further, the IRS internally recognizes that critical and high vulnerabilities are not remediated timely.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization has prepared and planned to meet the goals of the TIC initiative, consistent with OMB Memorandum M-19-26.[7] Specifically, the agency has defined and customized, as appropriate, its policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB Memorandum M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays. The agency has defined processes to develop and maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.

    Comments: The IRS provided evidence to support that an inventory is maintained of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection. However, the IRS needs to ensure that the information maintained is accurate and complete.

24. To what extent does the organization use a vulnerability disclosure policy as part of its vulnerability management program for internet-accessible federal systems?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently implements its vulnerability disclosure policy. In addition, the organization has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public; ensures that all internet-accessible systems are included in the scope of its vulnerability disclosure policy; and increases the scope of systems covered by its vulnerability disclosure policy, in accordance with the Department of Homeland Security, Binding Operational Directive 20-01.[8]

    Comments: The IRS provided reports to support its vulnerability disclosure program on a quarterly basis to the Department of the Treasury. Further, the IRS has leveraged the bug bounty initiative to identify vulnerabilities as suggested by OMB Memorandum M-20-32.[9] However, the IRS has not integrated the data into its internal management reporting process.

PROTECT Function Area – Identity and Access Management

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

    Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities.

[7] OMB, Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative* (Sept. 12, 2019).

[8] Department of Homeland Security, Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy* (Sept. 2, 2020).

[9] OMB, Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation* (Sept. 2, 2020).

Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

27. To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization is consistently implementing its ICAM policy, strategy, process, and technology solution roadmap and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the Federal ICAM and Continuous Diagnostics and Mitigation requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and roadmap and making updates as needed.

    Comments: While the IRS has consistently implemented its ICAM policies, procedures, and strategy, the evidence provided by the IRS was not sufficient to justify that the IRS integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. In addition, while the IRS provided examples of automated mechanisms, the evidence did not substantiate that the IRS uses automated mechanisms (*e.g.*, machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy.

29. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained?

    Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.

30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms *(e.g.*, Personal Identity Verification (PIV), Fast Identity Online 2, or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?[10]

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization’s facilities [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances in which it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided the option of using phishing-resistant multifactor authentication.

[10] Fast Identity Online 2 security model eliminates the risks of phishing, all forms of password theft, and replay attacks.

Comments: The IRS has implemented multifactor authentication mechanisms with PIV for personnel to access the organization's facilities at designated entry/exit points in 113 (34 percent) of the 335 buildings that require Enterprise Physical Access Control Systems, as of April 12, 2023. The projected completion plan for the remaining upgrades to the buildings is in Fiscal Year 2026. In addition, the IRS is in the process of implementing multifactor authentication to meet the requirements outlined in Executive Order 14028.

31. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (*e.g.*, PIV, Fast Identity Online 2, or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets. For instances in which it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.

    Comments: The IRS is in the process of implementing multifactor authentication to meet the requirements outlined in Executive Order 14028. The IRS has an open program-level POA&M for the IRS to implement and enforce multifactor authentication for all system components within the High Value Asset boundary.[11] According to the IRS, it is deploying an infrastructure that will provide multifactor authentication for all mainframe-based systems and applications.

32. 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?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; and ensures that privileged user activities are logged and periodically reviewed.

    Comments: The IRS migrated to a new system that provides the capability to manage privileged and elevated access to servers, mainframes, and network devices using privileged accounts. The IRS continues to identify and onboard privileged unmanaged accounts. In addition, the IRS indicated that it has increased the number of accounts identified as privileged by 40 percent, which is a 10 percent increase from last year.

33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of

[11] The IRS defines a High Value Asset as the IRS's most sensitive and critical systems needed to carry out its given mission.

appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions.

Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization ensures that Federal Information Processing Standards 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.

Comments: The *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics* lists OMB Memorandum M-22-09, as a criteria for this metric.[12] This memorandum sets forth a Federal Zero Trust Architecture strategy requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024. While the full Zero Trust Architecture implementation is not required until Fiscal Year 2024, TIGTA reported that the IRS has completed several activities including developing a reference architecture plan and roadmap. However, the IRS did not have a consolidated Fiscal Year 2024 budget estimate for the Zero Trust Architecture initiatives as required by OMB Memorandum M-22-09. According to the IRS Zero Trust Architecture Plan, a budget did not exist because the IRS needed to fully understand the remaining scope to complete each task before preparing a budget estimate of Zero Trust Architecture initiatives. In addition, the IRS did not accurately assess its zero-trust maturity.

PROTECT Function Area – Data Protection and Privacy

35. To what extent has the organization developed a privacy program for the protection of personally identifiable information that is collected, used, maintained, shared, and disposed of by information systems?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined and communicated its privacy program plan and related policies and procedures for the protection of personally identifiable information that is collected, used, maintained, shared, and/or disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of the organization's privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.

    Comments: The IRS provided a privacy program plan and procedures for protection of personally identifiable information; however, TIGTA reported that not all privacy controls have been fully implemented or assessed.

36. To what extent has the organization implemented the following security controls to protect its personally identifiable information and other agency sensitive data, as appropriate, throughout the data lifecycle (encryption of data at rest, encryption of data in transit, limitation of transfer to removable media, and sanitization of digital media prior to disposal or reuse)?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization's policies and procedures have been defined and communicated for the specific areas. Further, the

[12] OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).

policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.

Comments: While the IRS has defined policies and procedures to protect its personally identifiable information, it has not met the requirements outlined in Executive Order 14028 directing agencies to use encryption to protect data at rest. The IRS is using a phased implementation approach to implement data at rest encryption. In addition, GAO reported that while the IRS made progress in addressing certain information system security control deficiencies, significant deficiencies exist concerning encryption. Further, the IRS has open POA&Ms documenting encryption weaknesses in a number of systems.

37. To what extent has the organization implemented security controls (*e.g.*, Endpoint Detection and Response) to prevent data exfiltration and enhance network defenses?

Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing and malware and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of personally identifiable information. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization uses e-mail authentication technology and ensures the use of valid encryption certificates for its domains. The organization consistently implements Endpoint Detection and Response capabilities to support host-level visibility, attribution, and response for its information.

Comments: The *Fiscal Years 2023–2024 Inspector General FISMA Reporting Metrics* lists the OMB, Memorandum M-21-07, as criteria for this metric.[13] This memorandum communicates the requirements for completing the operational deployment of Internet Protocol Version 6 across all Federal information systems and services. According to the IRS, it is working through several dependencies to fully test and stand up the Internet Protocol Version 6 only environment. For requirements permitting only verified software to execute, the IRS uses a privilege manager platform to block executions of unauthorized software on endpoints. However, TIGTA reported that the methodology used to manage unauthorized software is not effectively managed.

PROTECT Function Area – Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

[13] OMB, Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6* (Nov. 19, 2020).

42. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.

    Comments: The IRS has not updated its knowledge, skills, and abilities assessment to account for a changing risk environment. However, according to the IRS, it is currently in the process of updating its knowledge, skills, and abilities assessment capabilities, and it anticipates that an interim Service-level automated competency/skills assessment will be available during the fourth quarter of Fiscal Year 2023. Also, the IRS has an open recommendation from a prior GAO report to fully implement information technology workforce planning practices.

43. To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment?

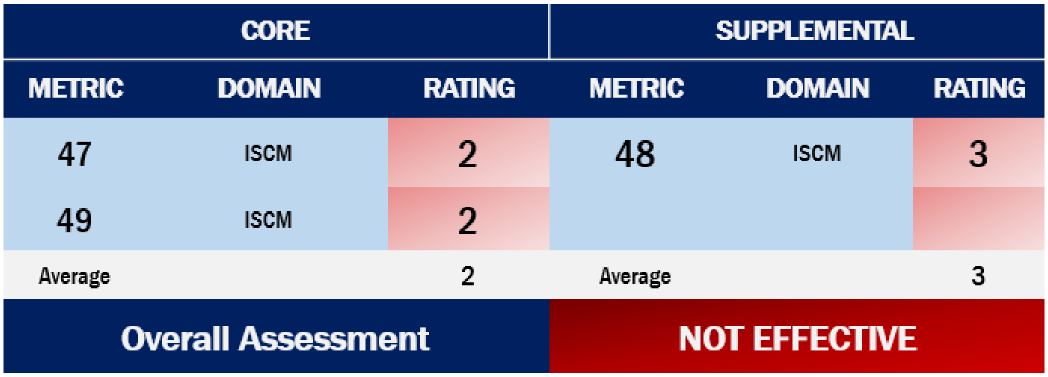
    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization has consistently implemented its organization-wide security awareness and training strategy and plan.

    Comments: Based on the information provided, we could not fully verify the existence of a Cybersecurity Workforce Assessment and associated gap analysis as described in the applicable FISMA criteria. However, based on the totality of available evidence, the metric was rated as Consistently Implemented. When evaluating the Managed and Measurable maturity level, there was insufficient evidence to support that data supporting the qualitative and quantitative measures used to determine the effectiveness of the security awareness and training strategies were obtained accurately, consistently, and in a reproducible format.

The Cybersecurity Framework function area of DETECT was rated as Not Effective

Based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, we found that the DETECT function area and the respective security program component, ISCM, met a Core maturity level of 2.0 and a Supplemental maturity level of 3.0, which we considered "not effective." Figure 6 presents the maturity level ratings for the assessed metrics.

Figure 6: Fiscal Year 2023 DETECT Function Area Assessment Results



CORE			SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
47	ISCM	2	48	ISCM	3
49	ISCM	2			
Average		2	Average		3
Overall Assessment			NOT EFFECTIVE		

Source: TIGTA's evaluation of security program metrics associated with the Cybersecurity Framework function area DETECT.

DETECT Function Area – Information Security Continuous Monitoring

47. To what extent does the organization use ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has developed, tailored, and communicated its ISCM policies and strategy. The following areas are included:

    - Monitoring requirements at each organizational tier.
    - The minimum monitoring frequencies for implemented controls across the organization. (The criteria for determining minimum frequencies are established in coordination with organizational officials [*e.g.*, senior accountable official for risk management, system owners, and common control providers] and in accordance with organizational risk tolerance).
    - The organization's ongoing control assessment approach.
    - How ongoing assessments are to be conducted.
    - Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy.

    Comments: The ISCM Program Plan indicates gaps in tools used to monitor hardware and software inventories. In addition, the plan includes outdated information. For example, the plan references NIST, Special Publication 800-53 Revision 4 instead of updated Revision 5, and policy checkers that are no longer used in the IRS. Further, the plan does not always provide or clearly state if tools used for maintaining various inventories are fully implemented. According to the IRS, it plans to update and finalize the ISCM Program Plan by June 2023.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

    Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – Individuals are performing roles and responsibilities that have been defined across the organization.

Comments: The IRS did not provide sufficient evidence to support allocation of resources (people, processes, and technology) in a risk-based manner.

49. 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?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans; monitoring security controls for individual systems; and time-based triggers for ongoing authorization. The system level strategy/policies address the monitoring of those controls that are not addressed by the organizational level strategy, as well as how changes to the system are monitored and reported.

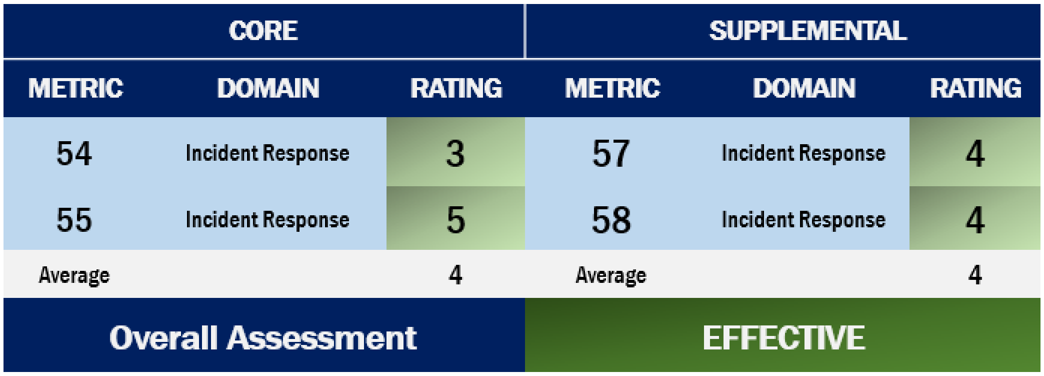
    Comments: While the IRS has defined its processes for performing ongoing security control assessments, it has not fully assessed NIST, Special Publication 800-53, Revision 5, controls to provide a view of the organizational security posture on FISMA systems. According to the IRS, it is on track to complete the NIST, Special Publication 800-53, Revision 5, control assessments by the Fiscal Year 2024 FISMA evaluation period. In addition, the Federal Risk and Authorization Management Program guidance is still operating under NIST, Special Publication 800-53, Revision 4; therefore, the IRS has not incorporated NIST, Special Publication 800-53, Revision 5, controls on its cloud systems.[14] Further, TIGTA reported that the privacy controls for on-premises and cloud systems were not fully assessed.

The Cybersecurity Framework function area of RESPOND was rated as Effective

Based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, we found that the RESPOND function area and the respective security program component, Incident Response, met a Core maturity level of 3.5 and a Supplemental maturity level of 4.0, which we considered "effective." Figure 7 presents the maturity level ratings for the assessed metrics.

[14] NIST, Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

Figure 7: Fiscal Year 2023 RESPOND Function Area Assessment Results



CORE			SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
54	Incident Response	3	57	Incident Response	4
55	Incident Response	5	58	Incident Response	4
Average		4	Average		4
Overall Assessment			EFFECTIVE		

Source: TIGTA's evaluation of security program metrics associated with the Cybersecurity Framework function area RESPOND.

RESPOND Function Area – Incident Response

54. How mature are the organization's processes for incident detection and analysis?

    Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.

    Comments: A new requirement for this metric is that the organization meets specific event logging requirements. However, based on our review of available information, we determined that the IRS needs to improve implementation of enterprise-wide event logging.

55. How mature are the organization's processes for incident handling?

    Maturity Level and Corresponding Narrative: ***Optimized (Level 5)*** – The organization uses dynamic reconfiguration (*e.g.*, changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.

57. To what extent does the organization collaborate with stakeholders to ensure that on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?

    Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – The organization uses Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.

58. To what extent does the organization use the following technology to support its incident response program?

    - Web application protections, such as web application firewalls.
    - Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools.

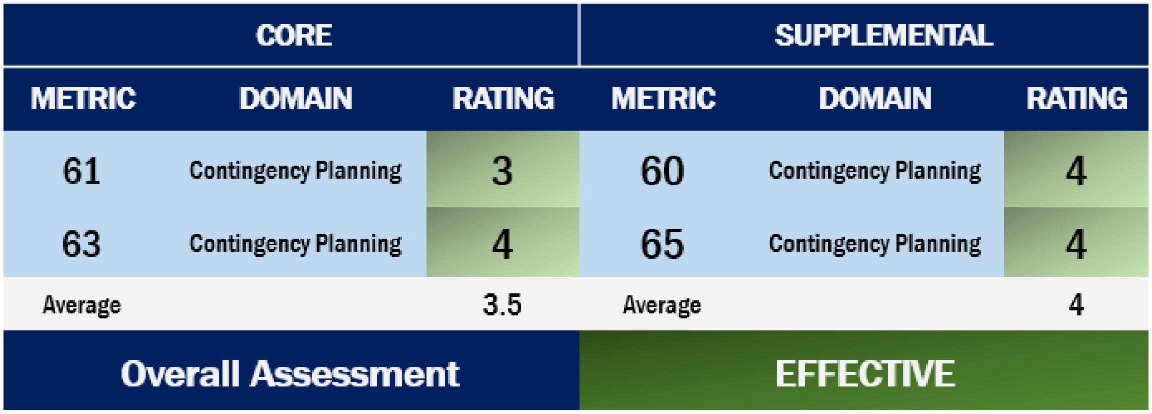
- Aggregation and analysis, such as security information and event management products.
- Malware detection, such as antivirus and antispam software technologies.
- Information management, such as data loss prevention.
- File integrity and endpoint and server security tools.

Maturity Level and Corresponding Narrative: *Managed and Measurable (Level 4)* -The organization evaluates the effectiveness of its incident response technologies and makes adjustments to configurations and toolsets, as appropriate.

The Cybersecurity Framework function area of RECOVER was rated as Effective

Based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*, we found that the RECOVER function area and the respective security program component, Contingency Planning, met a Core maturity level of 3.5 and a Supplemental maturity level of 4.0, which we considered "effective." Figure 8 presents the maturity level ratings for the assessed metrics.

Figure 8: Fiscal Year 2023 RECOVER Function Area Assessment Results



CORE			SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
61	Contingency Planning	3	60	Contingency Planning	4
63	Contingency Planning	4	65	Contingency Planning	4
Average		3.5	Average		4
Overall Assessment			EFFECTIVE		

Source: TIGTA's evaluation of security program metrics associated with the Cybersecurity Framework function area RECOVER.

RECOVERY Function Area – Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

    Maturity Level and Corresponding Narrative: *Managed and Measurable (Level 4)* – Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

    Maturity Level and Corresponding Narrative: *Consistently Implemented (Level 3)* - The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include characterization of all system components;

determination of missions/business processes and recovery criticality; identification of resource requirements; and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.

Comments: The IRS consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. However, the IRS did not provide evidence to support that it uses BIA results in conjunction with its risk register to calculate potential losses and inform senior level decision-making. Therefore, the IRS did not meet the *Managed and Measurable* maturity level.

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (*e.g.*, information and communications technology supply chain partners/providers), as appropriate.

65. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?

Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** – Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program on a maturity model spectrum based on the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics*. To accomplish our objective, we:

- Determined the maturity level for 20 core metrics and 20 supplemental metrics contained in the *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics* that pertain to the Cybersecurity Framework and related domains:
  - IDENTIFY (Risk Management and Supply Chain Risk Management).
  - PROTECT (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training).
  - DETECT (ISCM).
  - RESPOND (Incident Response).
  - RECOVER (Contingency Planning).
- Determined the rating of the Fiscal Year 2023 Inspector General 20 core metrics and 20 supplemental metrics by evaluating program documentation and interviewing key subject matter experts. We determined the information security program rating by applying a calculated average. The *Fiscal Years 2023-2024 Inspector General FISMA Reporting Metrics* allowed for some discretion on maturity level rating based on other considerations.
- Selected and evaluated a representative subset of seven IRS information systems. To select the systems, TIGTA followed the selection methodology that the Treasury Office of Inspector General defined for the Treasury Department as a whole. We used the information system inventory contained within the Treasury FISMA Inventory Management System. As of October 4, 2022, the Treasury FISMA Inventory Management System contained an IRS inventory of 85 general support systems and major applications considered operational with high and moderate security ratings. We used a random number table to select information systems within this population. Generally, if an information system was selected that was selected in the past three FISMA reviews, we reselected for that system.
- Considered the results of TIGTA audits applicable to FISMA metrics that were performed, completed, or contained recommendations that were still open during the Fiscal Year 2023 FISMA evaluation period as well as audit reports from the GAO that contained results applicable to FISMA metrics.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity function located in the New Carrollton Federal Building in Lanham, Maryland, during the period November 2022 through June 2023. We conducted this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Midori Ohno, Audit Manager; Charles Ekunwe, Senior Auditor; Charlene Elliston, Senior Auditor; Steven Stephens, Senior Auditor; Joyce Ajanaku, Auditor; and Laura Christoffersen, Data Analyst, Applied Research and Technology Division.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of the POA&M data obtained from the Treasury FISMA Inventory Management System website. We evaluated the data by 1) ensuring that the information was legible and contained alphanumeric characters; 2) reviewing required data elements; and 3) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined that the data were sufficiently reliable for the purpose of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our evaluation objective: Executive Order 14028; OMB memoranda; NIST, Special Publication 800 series; and Internal Revenue Manual policies related to information technology security controls. We evaluated these controls by reviewing documentation provided by the Cybersecurity function, interviewing IRS subject matter experts, and comparing relevant data and evidence obtained to the *Fiscal Years 2023-2024 Inspector General FISMA Metrics Evaluator's Guide* provided by the Council of the Inspectors General on Integrity and Efficiency, in coordination with the OMB, the DHS, and the Federal Chief Information Officers and Chief Information Security Officers councils.

Appendix II

Information Technology Security-Related Audits Considered During Our Fiscal Year 2023 Evaluation and the Metric(s) to Which They Apply

1. TIGTA, Report No. 2021-20-066, *The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement* (Sept. 2021) – Metric 36.
2. TIGTA, Report No. 2022-20-006, *Vulnerability Scanning and Remediation Processes Need Improvement* (Dec. 2021) – Metric 8.
3. TIGTA, Report No. 2022-27-028, *The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed* (May 2022) – Metrics 8 and 21.
4. TIGTA, Report No. 2022-20-065, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls* (Sept. 2022) – Metric 8.
5. TIGTA, Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (Mar. 2023) – Metric 21.
6. TIGTA, Report No. 2023-20-013, *The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed* (Mar. 2023) – Metric 21.
7. TIGTA, Report No. 2023-25-017, *Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement* (Apr. 2023) – Metric 37.
8. TIGTA, Report No. 2023-20-034, *Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed* (June 2023) – Metrics 35 and 49.
9. TIGTA, Report No. 2023-20-039, *Actions Are Needed to Improve the Zero Trust Architecture Implementation* (July 2023) – Metrics 10 and 33.
10. GAO, GAO-18-298, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 28, 2018) – Metric 42.
11. GAO, GAO-23-105564, *IRS's FY 2022 and FY 2021 Financial Statements* (Nov. 10, 2022) – Metrics 20 and 36.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

July 7, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Acting Chief Information Officer

2J6PB Digitally signed by 2J6PB
Date: 2023.07.07
14:16:47 -04'00'

SUBJECT: Draft Audit Report – Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation (Audit #202320001)

Thank you for the opportunity to review and comment on the discussion draft audit report. The IRS is committed to continuously improving our information security programs in accordance with the Federal Information Security Act of 2014 (FISMA) and ensuring a fully effective Cybersecurity Program with all program components at an acceptable maturity level.

While the IRS agrees that the Cybersecurity Framework function area of RESPOND is effective, we disagree with some aspects of the assessment in this area. Specifically, we do not concur with the assessment that the IRS has not fully implemented Event Logging Tier 2 (Intermediate) enterprise-wide in accordance with the Office of Management and Budget, Memorandum M-21-31. We provided evidence to confirm that on February 27, 2023, the IRS achieved the required Intermediate level for event logging. The IRS has increased its audit trail event logging to approximately 2.3 billion audit trail events per month compared to 953 million per month in February 2022. This 141% increase in the collection of audit trail events directly improves the detection and investigation of potential unauthorized accesses and violations of IRS security policies.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Cara Garr, Director of Security Risk Management, at (801) 620-4140.

Attachment

Appendix IV

Office of Audit Comment

In the IRS response to this report, management disagreed with our assessment regarding their Event Logging maturity rating. OMB Memorandum M-21-31 established an Event Logging maturity model that includes four tiers, from tier zero to tier three, and established due dates for Federal agencies to meet the requirements to attain each maturity level. The Event Logging maturity rating required by the OMB directly corresponded with maturity levels within Metric 54 of our review. For example, to rate the IRS *Consistently Implemented* in Metric 54, we would have to agree that the IRS was at Event Logging 1; to rate the IRS *Managed and Measurable*, we would have to determine that the IRS was at Event Logging 2. However, based on our review of available information, the IRS has not fully met the intent of implementing enterprise-wide event logging.

During Fiscal Year 2023, we conducted a separate review to determine whether the IRS effectively implemented an enterprise-wide audit management system that centralizes, standardizes, and provides better visibility and analysis capability for audit data from various sources to meet Federal and IRS requirements. That review discusses, in greater detail, the findings and conclusions we make regarding the IRS Event Logging maturity level, along with recommendations for improvements. The results of that audit will be issued in September 2023.

Appendix V

Abbreviations

BIA	Business Impact Analysis
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
ICAM	Identity, Credential, and Access Management
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SCRM	Supply Chain Risk Management
TIC	Trusted Internet Connection
TIGTA	Treasury Inspector General for Tax Administration

**To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via email at
oi.govreports@tigta.treas.gov.**

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.