

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Fiscal Year 2024 IRS Federal Information Security Modernization Act Evaluation

July 29, 2024

Report Number: 2024-200-039

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 2023, the IRS collected nearly \$4.7 trillion in gross taxes and processed almost 271.5 million tax returns and other forms, 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.

What TIGTA Found

The IRS Cybersecurity Program was generally aligned with applicable FISMA requirements and related policies and standards. However, due to program components that were not at an acceptable maturity level, the Cybersecurity Program was not fully effective based on the FISMA reporting metrics for Fiscal Years 2023 and 2024. The FISMA reporting metrics scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

In Fiscal Year 2023, TIGTA evaluated 20 core reporting metrics and 20 supplemental metrics. In Fiscal Year 2024, TIGTA continued to test the 20 core reporting metrics as well as the remaining 17 supplemental metrics and nine additional editorial metrics that were not evaluated in Fiscal Year 2023. The nine additional editorial metrics were used to cite information on the positive or negative effectiveness of the IRS Cybersecurity program areas.

Based on Fiscal Years 2023 and 2024 FISMA evaluations, three Cybersecurity Framework function areas at the IRS were "not effective" and two were "effective." The IDENTIFY (Risk Management and Supply Chain Risk Management), PROTECT (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), and DETECT (Information Security Continuous Monitoring) capabilities were "not effective" and the RESPOND (Incident Response) and RECOVER (Contingency Planning) capabilities were "effective" based on a *Managed and Measurable*, Level 4 rating.

The IRS continues to be not effective in the same program areas. 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; implementing flaw remediation on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its systems and facilities.

Without a security program in compliance with FISMA requirements, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

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.

TIGTA reviewed the FISMA reporting metrics for Fiscal Years 2023 and 2024 and found:

 The IRS Cybersecurity Program was considered **not fully effective**.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

July 29, 2024

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

A handwritten signature in cursive script, reading "Danny R. Verneuille".

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Fiscal Year 2024 IRS Federal Information Security
Modernization Act Evaluation (Audit No.: 2024200001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act¹ evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2024. 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 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 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protection of 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.

If you have questions, please contact me or Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

¹ 44 U.S.C. § 3551-3558 (2018).

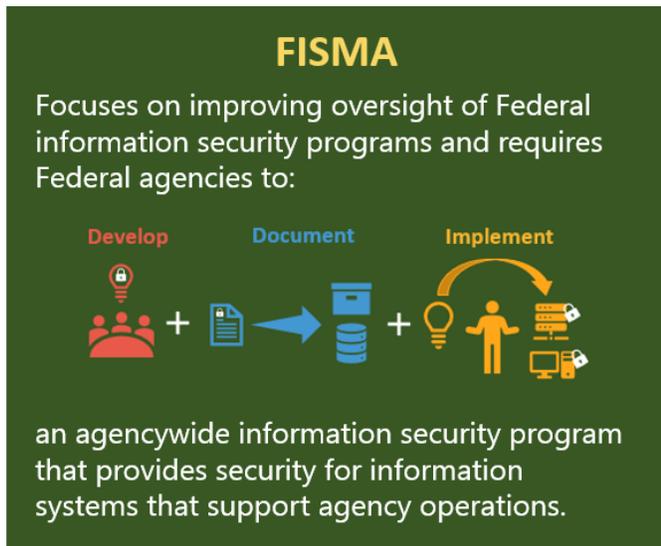
Table of Contents

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 4
<u>The Cybersecurity Program Was Not Effective in Three of the Five Function Areas</u>	Page 4
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 28
<u>Appendix II – Information Technology Security-Related Audits Considered During Our Fiscal Year 2024 Evaluation and the Metrics to Which They Apply</u>	Page 30
<u>Appendix III – Abbreviations</u>	Page 31

Background

The Federal Information Security Modernization Act of 2014 (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. FISMA assigns specific responsibilities to agency heads and Inspectors General in complying with its requirements 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.



For example, FISMA directs Federal agencies to report annually to the OMB, 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 (hereafter referred to as the Treasury Department) 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 2023, the IRS collected nearly \$4.7 trillion in gross taxes and processed almost 271.5 million tax returns and other forms, which represents a substantial amount of taxpayer personal and financial information. As the custodian of taxpayer information, the IRS is

¹ 44 U.S.C. § 3551-3558 (2018).

responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss.

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.

FISMA Reporting Metrics

The FISMA reporting metrics for Fiscal Years 2023-2024 were developed as a collaborative effort among 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 Officers' and Chief Information Security Officers' councils.²

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 20 core metrics that must be evaluated annually. These 20 core reporting metrics are a subset of the 66 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, *Improving the Nation's Cybersecurity*, and OMB cybersecurity guidance.³

In Fiscal Year 2023, the FISMA reporting metrics represented 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.

For Fiscal Year 2024, the Inspectors General will continue to test the 20 core reporting metrics as well as the remaining 17 supplemental metrics and nine additional editorial metrics that were not evaluated in Fiscal Year 2023. TIGTA used the nine additional editorial metrics to cite information on the effectiveness of the IRS Cybersecurity program areas and did not require a maturity level determination. According to the OMB, historically, the findings of Inspector General evaluations were released alongside annual reporting in October, but the agency assessed may not receive funding to remediate any problems identified until two or more years after the date of the report.⁴ To help remedy this situation, starting in Fiscal Year 2022, the OMB

² *Fiscal Year 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Feb. 2023).

³ Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021) and OMB Memoranda: M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 2021); M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (Oct. 2021); M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 2022); and M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 2022).

⁴ OMB, Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 2023).

shifted the due date of the metrics from October to July to better align the release of the evaluation with the development of the President’s Budget.

The FISMA reporting metrics align with the five cybersecurity function areas in the NIST’s *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter referred to as the Cybersecurity Framework).⁵ Figure 1 presents the five Cybersecurity Framework function areas and aligns each with the associated security program components (or metric domains).

Figure 1: Alignment of the Cybersecurity Framework Function Areas to the FISMA Reporting Metric Domains

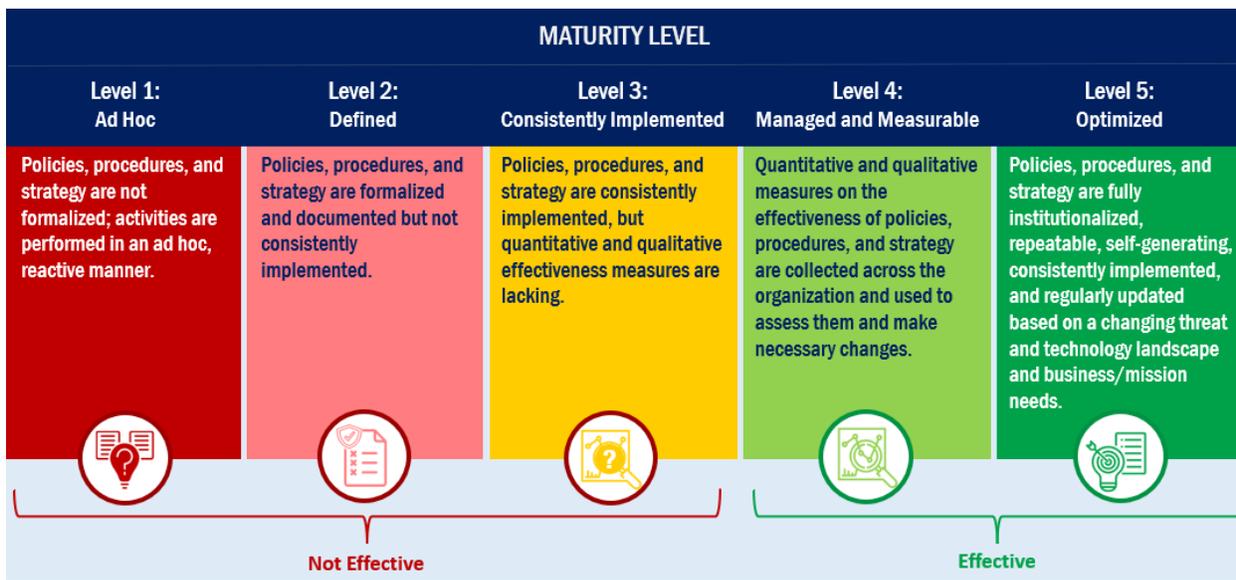
1 IDENTIFY 	2 PROTECT 	3 DETECT 	4 RESPOND 	5 RECOVER 
Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Develop and implement the appropriate activities 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: FISMA reporting metrics and the Cybersecurity Framework.

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.

⁵ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 2018).

Figure 2: FISMA Assessment Maturity Levels



Source: FISMA reporting metrics.

The Inspectors General were directed to 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 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 Cybersecurity Program Was Not Effective in Three of the Five Function Areas

The 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 fully effective. As shown in Figure 3, we rated three Cybersecurity Framework function areas as “not effective” and two as “effective.” The IDENTIFY, PROTECT, and DETECT capabilities were not effective and the RESPOND and RECOVER capabilities were effective. Figure 3 also includes the overall Cybersecurity Framework function areas ratings averaged independently to determine the assessed maturity.

Figure 3: Cybersecurity Framework Assessment Results

Functions	CORE	Fiscal Year 2023 SUPPLEMENTAL METRICS	Fiscal Year 2024 SUPPLEMENTAL METRICS	ASSESSED MATURITY
IDENTIFY	2.8	2.6	3.0	NOT EFFECTIVE
PROTECT	2.8	3.1	2.9	NOT EFFECTIVE
DETECT	2.0	3.0	2.0	NOT EFFECTIVE
RESPOND	4.0	4.0	3.7	EFFECTIVE
RECOVER	4.0	4.0	3.5	EFFECTIVE
Overall Maturity				NOT EFFECTIVE

Source: TIGTA’s evaluation of security program metrics.

The IRS continues to be evaluated as not effective in the same program areas. As examples of specific metrics that were considered not effective, we 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; implementing flaw remediation on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its systems and facilities. 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, the implementation status of key security controls, and TIGTA and Government Accountability Office (GAO) audit reports. These were reports that had results applicable to FISMA metrics, such as open recommendations, during the FISMA evaluation period of July 1, 2023, to June 14, 2024.⁶

Without a security program in compliance with FISMA requirements, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

The detailed results of our evaluation of the maturity level for each metric are provided below. The metrics are based on Federal Government guidance and criteria, an Executive Order, and OMB memoranda.⁷ For metrics rated lower than a maturity level 4, *Managed and Measurable*, we 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 FISMA reporting metrics.

The IDENTIFY function area was Not Effective

Based on the 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

⁶ See Appendix II for a list of these audits with notations as to which metrics the reports applied.

⁷ NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020); Executive Order 14028; and OMB Memoranda including the additional M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (Aug. 2021).

maturity level of 2.8 and a supplemental maturity level of 3.0, which we considered “not effective.” Figure 4 presents the maturity level ratings for the assessed metrics.

Figure 4: Fiscal Year 2024 IDENTIFY Function Area Assessment Results

CORE			Fiscal Year 2024 SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
1	Risk Management	3	4	Risk Management	4
2	Risk Management	2	6	Risk Management	3
3	Risk Management	2	15	SCRM	2
5	Risk Management	4			
10	Risk Management	3			
14	SCRM	3			
Average		2.8	Average		3.0
Overall Assessment			NOT EFFECTIVE		

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

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, it did not provide evidence to show that it maintains a comprehensive and accurate inventory of its information systems. The IRS is planning to renew an Interconnections System Agreement which expired in October 2019. In addition, we reported that the IRS does not have an accurate inventory of cloud applications. Although the IRS took corrective actions and designated a system of record for the cloud inventory applications, the finding identified cloud applications in the cloud inventory report that were not included in the designated system of record.

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?

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 fully implemented the hardware management tool according to the Information Security Continuous Monitoring (ISCM) Program Plan. In addition, the IRS has an open Plan of Action and Milestones (POA&M) related to being unable to detect unauthorized hardware, software, and firmware components and notify appropriate organizational officials.

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

Comments: According to the IRS, the software asset management tool is in the deployment stage of implementation. When the tool is fully deployed, the IRS will be able to detect unauthorized software. In addition, the IRS has an open POA&M stating it does not currently have a tool that prevents program execution in accordance with a list of authorized software programs, list of unauthorized software programs, and rules authorizing the terms and conditions of software program usage. Further, a GAO report analysis showed that the IRS legacy software is at least four versions behind the current version, with some instances behind 15 versions.

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?

Maturity Level and Corresponding Narrative: **Managed and Measurable (Level 4)** - The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.

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: **Managed and Measurable (Level 4)** – The organization uses the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment is documented in a cybersecurity risk register and serves as an input into the organization’s enterprise risk management program. The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are

maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to quantify and aggregate security risks, normalize cybersecurity risk information across organizational units, and prioritize operational risk response.

6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organization's information security architecture prior to introducing information system changes into the organization's environment. In addition, the organization employs a software assurance process for mobile applications.

Comments: The IRS made progress on addressing deficiencies in managing risk from the organization's supply chain since the Fiscal Year 2021 FISMA assessment. Specifically, the IRS finalized its SCRM Strategy Plan and formally launched its SCRM Program in October 2023. As of April 2024, the IRS conducted 47 rapid assessments for its critical third-party vendors. The IRS is beginning to conduct initial assessments of third-party vendors, which will provide a much more thorough assessment of a vendor's risk profile.

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 OMB requires agencies to achieve specific goals to achieve zero trust security by the end of Fiscal Year 2024. In May 2024, the IRS stated that it is on track to complete all actions required by the OMB by the end of Fiscal Year 2024. However, it has not yet provided sufficient evidence to support a *Managed and Measurable* rating. For example, the Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model documents five maturity model pillars along with four stages of implementation and guidance for measuring an agency's progress. One of the criteria for an agency to be at the Advanced stage of the Identity pillar is to authenticate all identities using phishing-resistant multifactor authentication. We reviewed the open POA&M report and found several open POA&Ms related to applications that were not in compliance with multifactor authentication. In addition, the IRS performed a Zero Trust Maturity Model assessment in March 2024 and rated six of the seven functions for the Identity pillar at the Initial stage.

11. Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported risk management program achievements:

- Improvements were made for how the Information System Security Officer role is established and maintained. A new official memorandum template was created that defines Information System Security Officers' roles and responsibilities, which they must read, understand, and sign. In addition, the IRS stated an enhanced Information System Security Officer training program was established for cloud and on-premise systems.
- The IRS modified the POA&M process and procedures to ensure that responsible owners are clearly advised of their roles and responsibilities regarding the timely creation, mitigation, and closing of the POA&Ms resulting from a TIGTA report recommendation.
- The IRS stated it created a high value asset compliance dashboard that shows the compliance metrics for all the Treasury Department defined high value assets.

Despite these Fiscal Year 2024 FISMA achievements, the IRS's risk management program has areas that need improvement, as follows:

- According to the IRS, it does not currently have risk snapshot information at the general support system level, but it is capturing risk information for the individual applications within a particular general support system. The IRS stated that it is working towards developing risk snapshot information for these systems by the end of Calendar Year 2024.
- Our review of the POA&Ms as of June 2, 2024, showed that the IRS had 1,233 active POA&Ms. We found that 395 (32 percent) of the 1,233 active POA&Ms were classified as late, while the remaining 838 (68 percent) were not late. Of the 395 that were classified as late, we found two critical, 50 high, 314 moderate, and 29 low risk severity POA&Ms. The 395 active POA&Ms have been classified as late from one to 3,076 days.

IDENTIFY Function Area – SCRM

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: **Consistently Implemented (Level 3)** – The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors, and system and system components. In addition, the organization obtains sufficient assurance, through audits, test results, software producer self-attestation (in accordance with OMB), or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Further,

the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.

Comments: According to the IRS, the SCRM Program went live in October 2023. The IRS began conducting Rapid and Initial Cybersecurity Supply Chain Risk Assessments. As of June 30, 2024, the IRS had completed 153 risk assessments for suppliers defined as critical that are currently in use. It conducted another 58 assessments for proposed third-party vendor procurements. The IRS has 95 Cybersecurity Supply Chain Risk Assessments planned through the end of Fiscal Year 2024 for critical and non-critical suppliers.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has defined and communicated its component authenticity policies and procedures. At a minimum the following areas are addressed:

- Procedures to detect and prevent counterfeit components from entering the system.
- Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.
- Requirements and procedures for reporting counterfeit system components.

Comments: The IRS updated its Internal Revenue Manual to include SCRM controls for Tamper Resistance and Detection as well as Component Authenticity.⁸ In addition, the SCRM Office has documented an SCRM Product Integrity Program Plan that established a two phased implementation plan with the initial phase placing priority on Tamper Resistance and Detection and Component Authenticity detection measures prior to the deployment of hardware, software, and firmware. The second phase includes Tamper Resistance and Detection and Component Authenticity measures to address hardware, software, and firmware risks after deployment. According to the IRS, it is targeting to complete Phase 1 by December 2024 and Phase 2 by June 2025. In addition, the Cybersecurity SCRM Program Office also developed and provided Tamper Resistance and Detection and Component Authenticity requirements introductions and training briefs to the members of the Cybersecurity SCRM Integrated Project Team which has representation from all Information Technology functions affected by the Product Integrity element of the Cybersecurity SCRM Program.

16. Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported SCRM achievements:

⁸ Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (Dec. 2022).

- The IRS conducted an internal audit on the effectiveness of Program security controls implementation. The results identified 19 program controls audited with 15 controls fully implemented and four controls partially implemented.
- The Cybersecurity SCRM Program Office procured and implemented an automated third-party risk management tool in October 2023 to support the Program’s “go live” event. The automated tool supports the Cybersecurity SCRM Program’s goal of providing consistently implemented supply chain risk assessments and continuous monitoring of IRS third-party vendors and service providers.

Despite these Fiscal Year 2024 FISMA achievements, the IRS’s SCRM program has the following example as an area that needs improvement:

- While the IRS has a Product Integrity Program Plan which supplements the enterprise-level Internal Revenue Manual requirements for Tamper Resistance and Detection and Component Authenticity, it lacks procedures to help IRS organizations with understanding and executing those requirements. According to the SCRM office, the goal is to have operational standard operating procedures drafted by December 1, 2024.

The PROTECT function area was Not Effective

Based on the 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 2.8 and a supplemental maturity level of 2.9, which we considered “not effective.” Figure 5 presents the maturity level ratings for the assessed metrics.

Figure 5: Fiscal Year 2024 PROTECT Function Area Assessment Results

CORE			Fiscal Year 2024 SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
20	Configuration Management	2	17	Configuration Management	3
21	Configuration Management	3	18	Configuration Management	2
30	Identity and Access Management	3	23	Configuration Management	2
31	Identity and Access Management	3	28	Identity and Access Management	3
32	Identity and Access Management	4	38	Data Protection and Privacy	4
36	Data Protection and Privacy	2	39	Data Protection and Privacy	3
37	Data Protection and Privacy	3	44	Security Training	3
42	Security Training	2	45	Security Training	3
Average		2.8	Average		2.9
Overall Assessment			NOT EFFECTIVE		

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

PROTECT Function Area – Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

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

Comments: While the IRS met maturity level 3, *Consistently Implemented*, the IRS did not specifically address allocation of resources in a risk-based manner to effectively perform information system configuration management activities. In addition, the IRS provided only the Authorizing Official and Information System Security Officer appointment letters for holding stakeholders accountable for carrying out their roles and responsibilities.

18. To what extent does the organization use an enterprise-wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board or related body; configuration management processes, including processes for identifying and managing configuration items during the appropriate phase within an organization's System Development Life Cycle; configuration monitoring; and applying configuration management requirements to contractor operated systems?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has developed an organization wide configuration management plan that includes the necessary components.

Comments: While the IRS developed an organization wide configuration management plan, it did not provide sufficient supporting documents to meet maturity level 3, *Consistently Implemented*. For example, using lessons learned to make improvements to the configuration management plans and activities is a requirement to meet maturity level 3, *Consistently Implemented*. To support this requirement, the IRS provided lessons learned documents for five (71 percent) of the seven sampled information systems; however, it did not record improvements to the configuration management activities and plans. For one (14 percent) of the seven sampled information systems, we agree that a lessons learned document was not required on a Software-as-a Service cloud system. For the remaining one (14 percent) of the seven sampled information systems, the IRS did not provide a lessons learned document.⁹ In addition, the IRS has an open program-level POA&M documenting that the general support systems did not demonstrate that security and privacy representatives are required to be members of the Configuration Change Control Board.

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,

⁹ Due to rounding the three percentages in this comment do not total to 100 percent.

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 defined configuration settings and common secure configurations, it has failed to provide security content automation protocol-validated software tools for one of the seven sampled information systems. The GAO reported that the IRS did not consistently implement security configuration settings for certain servers supporting systems significant to financial statements; however, the IRS stated that it is in the process of submitting documents to close the recommendations. In another report, the GAO reported that the new and continuing deficiencies include management of configuration settings for certain platforms.

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: **Consistently Implemented (Level 3)** – The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and uses lessons learned in implementation to make improvements to its flaw remediation policies and procedures. Further, for Executive Order-critical software platforms and all software deployed to those platforms, the organization uses support software versions.

Comments: While the IRS has policies, procedures, and processes for flaw remediation, the IRS System Security and Privacy Plan for IRS Organizational Common Controls states that the Cybersecurity function is not performing credentialed vulnerability scanning on mainframe operating systems. In addition, we reported that some known exploited vulnerabilities are not remediated timely. However, the FISMA reporting metrics allow for some discretion on maturity level ratings and based on the IRS having lessons learned regarding their flaw remediation processes, we rated this program area at maturity level 3, *Consistently Implemented*.

23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system, documentation of configuration change decisions, implementation of approved configuration changes, retaining records of implemented changes, auditing and review of configuration changes, and coordination and oversight of changes by the Control Change Board, as appropriate?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address at a minimum, the necessary configuration change control related activities.

Comments: The IRS is using a Change Management Procedure dated April 2017 that references a change management tool no longer used by the IRS. In addition, the IRS has multiple open POA&Ms referencing weaknesses in configuration change controls. Further, the IRS has a configuration management risk-based decision that was approved in

September 2018; however, steps were not taken to renew the risk-based decision in accordance with IRS policy.

25. Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported configuration management program achievements:

- The IRS replaced a configuration change control system with an automated process.
- The Configuration Management tool vulnerability dashboard was integrated with the security information and event management tool.

Despite these Fiscal Year 2024 FISMA achievements, the IRS's configuration management program has the following example of an area that needs improvement.

- Specific servers are not in compliance with configuration requirements. Specifically, configuration vulnerability age is not tracked, checklists used in the configuration compliance scanning tool are outdated, and differences in requirements are not documented.

PROTECT Function Area – Identity and Access Management

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?

Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.

Comments: We reported that the IRS did not always remove contractor access to sensitive systems when background investigations were not favorable, and three contractors did not have any active contracts with the IRS and retained their network and system access. According to the IRS, it is moving quickly to resolve the findings from the audit.

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?

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.

Comments: IRS personnel stated the IRS does not have a centrally supported non-PIV authentication mechanism to support maturity level 4, *Managed and Measurable*. Further, the IRS has an open recommendation from a prior TIGTA report to ensure that all noncompliant card readers (to access the IRS's facilities) are replaced with Federally compliant card readers and are properly configured.

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: According to IRS personnel, the IRS has completed implementation of multifactor authentication in support of Executive Order 14028 for seven high value assets as of December 2023; however, 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. The IRS also stated that it is working towards multifactor authentication compliance for 24 (14 percent) of 172 systems. The remaining 148 (86 percent) systems are compliant. Of the 24 noncompliant systems, two are considered high value assets.

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: **Managed and Measurable (Level 4)** - The organization employs automated mechanisms (e.g., machine-based or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. Further, the organization is meeting privileged identity and credential management logging requirements at maturity Event Logging 2, in accordance with the OMB.

34. Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 review. We selected some examples from these

IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported identity and access management program achievements:

- The IRS has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to granting access to systems. Processes are defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, and authorizing access after screening completion.
- The IRS documented that it has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including the completion of digital identity risk assessments.

Despite these Fiscal Year 2024 FISMA achievements, the IRS's identity and access management program has the following example of an area that needs improvement:

- According to the IRS, it has built a well-established process for monitoring user behavior to detect potential insider threats originating from either intentional or inadvertent misuses of taxpayer information. In addition, the IRS claimed it implemented streamlined procedures for IRS Cybersecurity personnel to immediately revoke user access to IRS systems to ensure protection of sensitive data. However, the information provided indicates that while the availability and timeliness of usable log information has improved, it does not substantiate that the IRS evaluates personnel security information from various sources on a near-real-time basis.

PROTECT Function Area – Data Protection and Privacy

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 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 still has not met the requirement to enforce Federal Information Processing Standards compliant encryption. According to IRS personnel, data on five (38 percent) of the 13 high value assets was not encrypted at rest, while the data on the remaining eight (62 percent) high value assets was encrypted at rest. The IRS has postponed encrypting the high value assets and may not meet the Treasury Department goal of October 1, 2024. The IRS expects high value assets to be fully encrypted by Fiscal Year 2025. In addition, the GAO reported that control deficiencies include encryption of sensitive data.

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: Although the OMB requires the IRS to have 20 percent of its Internet Protocol-enabled assets operating in Internet Protocol version 6-only environments by the end of Fiscal Year 2023, the IRS reported that less than 1 percent were operating in that environment as of March 2024.¹⁰ In addition, according to the IRS, it is working with the Treasury Department on mobile endpoint detection and response requirements to provide answers not only for the IRS, but also all other Treasury Department bureaus.

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

Maturity Level and Corresponding Narrative: **Managed and Measurable (Level 4)** – The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibility for Personally Identifiable Information or activities involving Personally Identifiable Information receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.

Comments: The IRS stated it does not measure the effectiveness of the privacy awareness training program by obtaining feedback on the content of the training. For privacy awareness training, the IRS provided Fiscal Year 2023 Employee Mandatory Briefings of its employees showing a 98 percent completion rate as of October 13, 2023. In addition, the IRS provided Fiscal Year 2023 Contractor Mandatory Briefings of its contractors showing a 77 percent completion rate as of March 27, 2024. The contractor's completion rate was below the Human Capital Office goal of 95 percent.

40. Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above.

¹⁰ OMB, Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6* (Nov. 19, 2020).

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported data protection and privacy program achievements:

- In July 2023, communications to all IRS employees and contractors were issued detailing the more stringent guidelines for use of removable media.
- In August 2023, Cybersecurity updated the procedures for requesting removable media access.

Despite these Fiscal Year 2024 FISMA achievements, the IRS's data protection and privacy program has the following example of an area that needs improvement.

- The IRS does not comply with OMB's mandate for the removal of TikTok from IRS devices because computers and mobile devices assigned to IRS employees continue to have the functionality to access TikTok and other related websites.

PROTECT Function Area – Security Training

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 defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updates its assessment to account for a changing risk environment.

Comments: According to IRS personnel, the revision of the assessment process of the knowledge, skills, and abilities of its workforce led to the identification of skill gaps. Most of the training options have yet to be assigned to the impacted employees. In addition, the IRS was unable to provide evidence to support the completion of Specialized Information Technology Security role-based training. Further, the IRS has an open recommendation from a prior GAO report to fully implement information technology workforce planning practices.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization ensures that its security awareness policies and procedures are consistently implemented. The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined time frames] and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.

Comments: The IRS did not provide sufficient evidence to support quantitative and qualitative performance measures on the effectiveness of its security awareness policies, procedures, and practices.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** - The organization ensures that its security training policies and procedures are consistently implemented. The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined time frames] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities. The organization obtains feedback on its security training program and uses that information to make improvements.

Comments: The IRS did not provide evidence that it measures the effectiveness of its specialized security training program; therefore, the IRS did not meet the *Managed and Measurable* maturity level. In addition, the IRS has a program-level POA&M on lessons learned from security threats that are not being integrated into role-based training curriculum.

46. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported security training program achievements:

- The IRS conducted two specific internal audits on contractors to ensure that their security awareness training is assigned and completed in the Integrated Talent Management training system of record.
- The IRS holds an annual interactive session providing specialized security training for the Chief Information Officer, Chief Information Officer's direct staff, and Information Technology Executives from across all Associate Chief Information Officer organizations. The presentations address the current threat landscape, near term process, tool updates, and how the other Associate Chief Information Officer areas can contribute to the strengthening and resiliency of the IRS network.

Despite these Fiscal Year 2024 FISMA achievements, the IRS's security training program has the following example of an area that needs improvement:

- The IRS's security awareness and training needs a mandatory security training program that drives literacy training and awareness, and its role-based training has not been aligned to the workforce assessment.

The DETECT function area was Not Effective

Based on the 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 2.0, which we considered “not effective.” Figure 6 presents the maturity level ratings for the assessed metrics.

Figure 6: Fiscal Year 2024 DETECT Function Area Assessment Results

CORE			Fiscal Year 2024 SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
47	ISCM	2	50	ISCM	2
49	ISCM	2			
Average		2.0	Average		2.0
Overall Assessment			NOT EFFECTIVE		

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

DETECT Function Area – ISCM

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 IRS has developed an ISCM Program Plan; however, the plan includes outdated information. The ISCM Program Plan states each FISMA reportable boundary must complete a point-in-time annual security controls assessment to validate a subset of the

applicable NIST security controls. The IRS has yet to update the ISCM Program Plan to reflect NIST revisions. Further, the ISCM Program Plan is missing a current software management tool used by the IRS and references a tool that has been replaced.

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 processes for performing information system assessments, it has not consistently implemented system level continuous monitoring strategies and related processes. The IRS has not fully tested security controls required by NIST to provide a view of the organizational security posture on FISMA systems. According to the IRS, all of its on-premise systems will be assessed with security control assessments from NIST by the conclusion of the Fiscal Year 2024 FISMA evaluation period. In addition, as of February 2024, all cloud assessments are being assessed utilizing NIST over a three-year period.

The February 2024 Enterprise FISMA dashboard shows 12 (7 percent) of the 162 IRS systems have an expired or past due annual security control assessment, three (2 percent) of the 162 systems had an expired or past due Information Systems Contingency Plan Test, and five (3 percent) of the 162 systems have an expired Privacy and Civil Liberties Impact Assessment. The remaining 142 systems (88 percent) did not have any of these three identified issues. The IRS stated that the February 2024 Enterprise FISMA dashboard information was not accurate and provided the March 2024 Enterprise FISMA dashboard and evidence to show that the dashboard does not reflect some of the late documents. Further, we reported that the IRS has not identified threat hunting security controls for inclusion in the Internal Revenue Manual based on NIST guidance.

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, the organization has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.

Comments: Although the IRS has evidence of collecting performance measures for continuous monitoring, two mechanisms for measuring performance have not been reported or defined. According to the IRS, it has not developed reports to support performance measures of the ISCM program and has no metrics to identify how the ISCM program delivers situational awareness.

51. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported ISCM program achievements:

- Security support roles, such as the Information System Security Officers to Authorizing Officials have been improved to support security efforts at the program level.
- Risks are reviewed prior to any system moving into production, thereby improving the overall risk posture of the IRS.
- The IRS's assessment teams have improved their activities to ensure that system risks are identified prior to the system being placed into production and during the annual assessment process.
- The Cyber dashboard reporting has improved and provides owners with near-real-time reporting to improve on remediation efforts.

Despite these Fiscal Year 2024 FISMA achievements, the ISCM program has the following areas that need improvement:

- The IRS did not ensure that all assessed privacy control results are correctly applied to all fields in the new assessment and monitoring system and captured in the system security plans.
- The IRS did not ensure that all NIST privacy controls for on-premise systems are implemented.

The RESPOND function area was Effective

Based on the FISMA reporting metrics, we found that the RESPOND function area and the respective security program component, Incident Response, met a core maturity level of 4.0 and a supplemental maturity level of 3.7, which we considered "effective." Figure 7 presents the maturity level ratings for the assessed metrics.

Figure 7: Fiscal Year 2024 RESPOND Function Area Assessment Results

CORE			Fiscal Year 2024 SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
54	Incident Response	3	52	Incident Response	4
55	Incident Response	5	53	Incident Response	4
			56	Incident Response	3
Average		4.0	Average		3.7
Overall Assessment			EFFECTIVE		

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

RESPOND Function Area – Incident Response

52. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

Maturity Level and Corresponding Narrative: **Managed and Measurable (Level 4)** – The organization monitors and analyzes the qualitative and quantitative performance measures that have been defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

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

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

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization consistently implements its policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management, antivirus and antispam software, and file integrity checking software. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary. In addition,

the organization is meeting logging requirements at maturity Event Logging 1 (basic), in accordance with OMB.

Comments: An IRS executive stated that IRS high value assets are meeting logging requirements at Event Logging 3 maturity level, and all other systems are meeting Event Logging 2 maturity level. In addition, the IRS formally documented a method of mapping OMB Event Logging requirements to demonstrate that compliance has been implemented and mapping is in process. This was documented via an update to the Joint Audit Management Enterprise System for an open recommendation from a prior TIGTA report, which was to implement a method of mapping the OMB requirements for all IRS systems to track and demonstrate compliance. However, there is a GAO report that identified continued deficiencies in logging and monitoring of audit records, as well as an open program-level POA&M stating that the IRS does not capture audit records from all systems. Despite these issues, we determined the IRS met maturity level 3, *Consistently Implemented*.

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.

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to the United States Computer Emergency Readiness Team, law enforcement, the Office of Inspector General, and Congress (for major incidents) in a timely manner. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.

Comments: The information supplied by the IRS was not sufficient to demonstrate that it is measuring or managing the timely reporting of incident information to stakeholders, or that data supporting metrics are obtained consistently, accurately, or in a reproducible format. The IRS did provide a narrative response describing certain processes to manage and measure incident reporting timeliness as well as how data is obtained and reviewed for accuracy. However, this information was only a narrative and there was little to no additional support to corroborate any of the information.

59. Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Examples of IRS-reported incident response program achievements:

- IRS Computer Security Incident Response Center regularly engages with one of its newer Cyber Operations teams, the Counter Insider Threat team. According to the IRS this is an essential relationship, as the line between network, endpoint, application, and user/identity security is becoming obscured. The Counter Insider Threat team, as a newer team, brings fresh eyes to some of these problems and offers incredible insights into new tools, techniques, and procedures for incident response, from its Insider Threat perspective.
- The IRS stated that the Computer Security Incident Response Center establishes and maintains relationships with organizations that may give potential early notification of indicators of concern. These organizations include teams from internal and external partners. In addition to receiving potential artifacts of cybersecurity concern, these partners are also valuable in putting certain issues or indicators of concern in perspective, thereby assisting with analysis.

The IRS did not have any TIGTA or GAO open recommendations relating to IRS’s incident response program.

The RECOVER function area was Effective

Based on the FISMA reporting metrics, we found that the RECOVER function area and the respective security program component, Contingency Planning, met a core maturity level of 4.0 and a supplemental maturity level of 3.5, which we considered “effective.” Figure 8 presents the maturity level ratings for the assessed metrics.

Figure 8: Fiscal Year 2024 RECOVER Function Area Assessment Results

CORE			Fiscal Year 2024 SUPPLEMENTAL		
METRIC	DOMAIN	RATING	METRIC	DOMAIN	RATING
61	Contingency Planning	4	62	Contingency Planning	4
63	Contingency Planning	4	64	Contingency Planning	3
Average		4.0	Average		3.5
Overall Assessment			EFFECTIVE		

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

RECOVER Function Area – Contingency Planning

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

Maturity Level and Corresponding Narrative: **Managed and Measurable (Level 4)** – The organization ensures that the results of organizational and system level business impact analyses are integrated with enterprise risk management processes, for consistently

evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its business impact analyses in conjunction with its risk register to calculate potential losses and inform senior level decision-making.

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

Maturity Level and Corresponding Narrative: **Managed and Measurable (Level 4)** – The organization can integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization. The organization coordinates the development of Information Systems Contingency Plans with the contingency plans of external service providers.

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.

64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization consistently implements its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and redundant array of independent disks, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites are not subject to the same risks as the primary site. Further, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site, including applicable Information and Communications Technology supply chain controls. Further, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.

Comments: To achieve maturity level 4, *Managed and Measurable*, the IRS stated it will continue to ensure that its backup and storage systems, including alternate storage and processing sites, are configured to facilitate recovery operations in accordance with recovery time and recovery point objectives. The IRS has several open POA&Ms related to the 12-hour recovery time objective and are working to close these POA&Ms to achieve compliance.

66. Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above.

Comments: The IRS supplied information about its noteworthy accomplishments and achievements during the Fiscal Year 2024 FISMA review. We selected some examples from these IRS-reported achievements. This information was not verified or evaluated during this review.

Example of an IRS-reported contingency planning program achievement:

- The IRS contingency planning team closed all seven recommendations from a prior TIGTA report on disaster recovery.

The IRS did not have any TIGTA or GAO open recommendations relating to IRS's contingency planning program.

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 Federal Information Security Modernization Act of 2014 Reporting Metrics*. To accomplish our objective, we:

- Evaluated the 20 core metrics as well as 17 supplemental metrics and nine additional editorial metrics that pertain to the Cybersecurity Framework and related domains that were not assessed in Fiscal Year 2023 by reviewing program documentation and interviewing key subject matter experts. We determined the information security program rating by applying a calculated average. The FISMA reporting metrics allowed for some discretion on maturity level rating based on other considerations. Some specific examples that allowed us to make these evaluations included the following:
 - Selected a representative subset of seven IRS information systems to evaluate the implementation status of key security controls. To select the systems, we 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 January 9, 2024, this system contained an IRS inventory of 98 general support systems and major applications considered operational with high and moderate security ratings. We used a random number generator 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.
 - Reviewed and analyzed a Treasury FISMA Inventory Management System report with 1,233 active POA&Ms as of June 2, 2024, to identify the risk severity levels and late POA&Ms. In addition, we evaluated the POA&Ms that document weaknesses at the IRS program and system levels for evaluating the metrics.
 - Assessed the status of GAO and TIGTA audit recommendations that were open during the FISMA evaluation period of July 1, 2023, through June 14, 2024. This was done by reviewing reports generated in the Joint Audit Management Enterprise System applicable to the FISMA reporting metrics.¹

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 January 2024 through June 2024. 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

¹ See Appendix II for a list of these audits with notations as to which metrics the reports applied.

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 Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Midori Ohno, Audit Manager; Daniel Preko, Audit Manager; Steven Stephens, Lead Auditor; Charles Ekunwe, Senior Auditor; Charlene Elliston, Senior Auditor; Shebrina Lewis, Senior Auditor; Michael Mohrman, Senior Auditor; Shanda Braxton, Auditor; Ruth Chen, Auditor; Komlanvi Komabane, Auditor; Chaquita Parker, Auditor; SaQoya Bennett, Student Intern; and Terrance Walton, Information Technology Specialist (Data Analytics).

Data Validation Methodology

During this review, we relied on security documents and the POA&MS in the Treasury FISMA Inventory Management System. We performed tests to assess the reliability of the system inventory and 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 the data were sufficiently reliable for the purpose of the 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 Department of Homeland Security, and the Federal Chief Information Officers' and Chief Information Security Officers' councils.

Appendix II

Information Technology Security-Related Audits Considered During Our Fiscal Year 2024 Evaluation and the Metrics to Which They Apply

1. TIGTA, Report No. 2023-20-023, *Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement* (May 2023) – Metric 66.
2. TIGTA, Report No. 2023-20-040, *The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved* (July 2023) – Metric 49.
3. TIGTA, Report No. 2023-20-042, *Security Weaknesses Are Not Timely Resolved and Effectively Managed* (Aug. 2023) – Metric 11.
4. TIGTA, Report No. 2023-20-062, *The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement* (Sept. 2023) – Metric 30.
5. TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (Oct. 2023) – Metric 54.
6. TIGTA, Report No. 2024-200-009, *Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements* (Jan. 2024) – Metric 1.
7. TIGTA, Report No. 2024-IE-R008, *Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information* (Feb. 2024) – Metric 28.
8. GAO, GAO-19-176, *Internal Revenue Service: Strategic Human Capital Management is Needed to Address Serious Risks to IRS's Mission* (Mar. 2019) – Metric 42.
9. GAO, GAO-23-104719, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements* (Jan. 2023) – Metric 3.
10. GAO, GAO-24-106472, *Financial Audit: IRS's FY 2023 and FY 2022 Financial Statements* (Nov. 2023) – Metrics 20, 36, and 54.
11. GAO, GAO-24-107185, *IRS Financial Reporting: Improvements Needed in Information System and Other Controls* (Apr. 2024) – Metric 20.

Appendix III

Abbreviations

FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
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
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 e-mail 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.