TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation

July 18, 2022

Report Number: 2022-20-040

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

HIGHLIGHTS: Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation

Final Audit Report issued on July 18, 2022 **Report Number 2022-20-040**

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 information security program on a maturity model spectrum based on the Fiscal Year 2022 Core Inspector General 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 2021, the IRS received and processed more than 261 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.

What TIGTA Found

For Fiscal Year 2022, 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).

The IRS's Cybersecurity Program was generally aligned with applicable FISMA requirements, Office of Management and Budget policy and guidance, and National Institute of Standards and Technology standards and guidelines.

For the 20 Fiscal Year 2022 Core Inspector General Metrics, TIGTA found one metric achieved the *Optimized* maturity level 5 and two metrics achieved the *Managed and Measurable* maturity level 4. However, TIGTA determined the Cybersecurity Program was not effective in 17 of the 20 metrics. Six metrics were at a *Consistently Implemented* maturity level 3 and 11 metrics were at a *Defined* maturity level 2.

Due to program components that were not at an acceptable maturity level, the Cybersecurity Program was not considered fully effective. The *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

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; maintaining secure configuration settings for its information systems; implementing flaw remediation and patching on a consistent and timely basis; and ensuring that security controls for protecting Personally Identifiable Information are fully implemented.

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 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.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

July 18, 2022

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 2022 IRS Federal Information Security Modernization Act Evaluation (Audit # 202220001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2022. 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 Year 2022 Core Inspector General Metrics. This audit is included in our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of 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.

Copies of this report are also being sent to the IRS managers affected by the report. If you have questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. 113-283.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 3

The Cybersecurity Program Was Not Effective in 17 of the 20 Fiscal Year 2022 Core Inspector General Metrics ..... Page 3

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 14

Appendix II – Information Technology Security-Related Audits Considered During Our Fiscal Year 2022 Evaluation and the Metric(s) to Which They Apply ..... Page 16

Appendix III – Abbreviations ..... Page 17

Background

The Federal Information Security Modernization Act of 2014,[1] hereafter referred to as FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. 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 requires Federal agencies to implement an agencywide information security program. It also requires agencies to have an annual independent evaluation performed of their information security programs and practices, generally performed by the agency's Inspector General.

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 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 2021, the IRS collected more than $4.1 trillion in gross taxes and processed more than 261 million Federal tax returns and supplemental documents, which represents a substantial amount of taxpayer personal and financial information. As custodians 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. 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

[1] Pub. L. No. 113-283.

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 the IRS systems and its data.

Fiscal Year 2022 Core Inspector General Reporting Requirements

The *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* was developed as a collaborative effort among representatives from the OMB, the Council of the Inspectors General on Integrity and Efficiency, the Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the Intelligence Community. The 20 Fiscal Year 2022 Core Inspector General Metrics represent a continuation of work begun in Fiscal Year 2016, when the Inspector General metrics were aligned with the five cybersecurity function areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, referred to as the Cybersecurity Framework.[2] The five Cybersecurity Framework function areas and 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).

The 20 Fiscal Year 2022 Core Inspector General Metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[3] as well as recent OMB guidance[4] to agencies in furtherance of the modernization of Federal cybersecurity. These 20 core reporting metrics are a subset of the 66 reporting metrics from the Fiscal Year 2021 Inspector General FISMA Reporting Metrics.

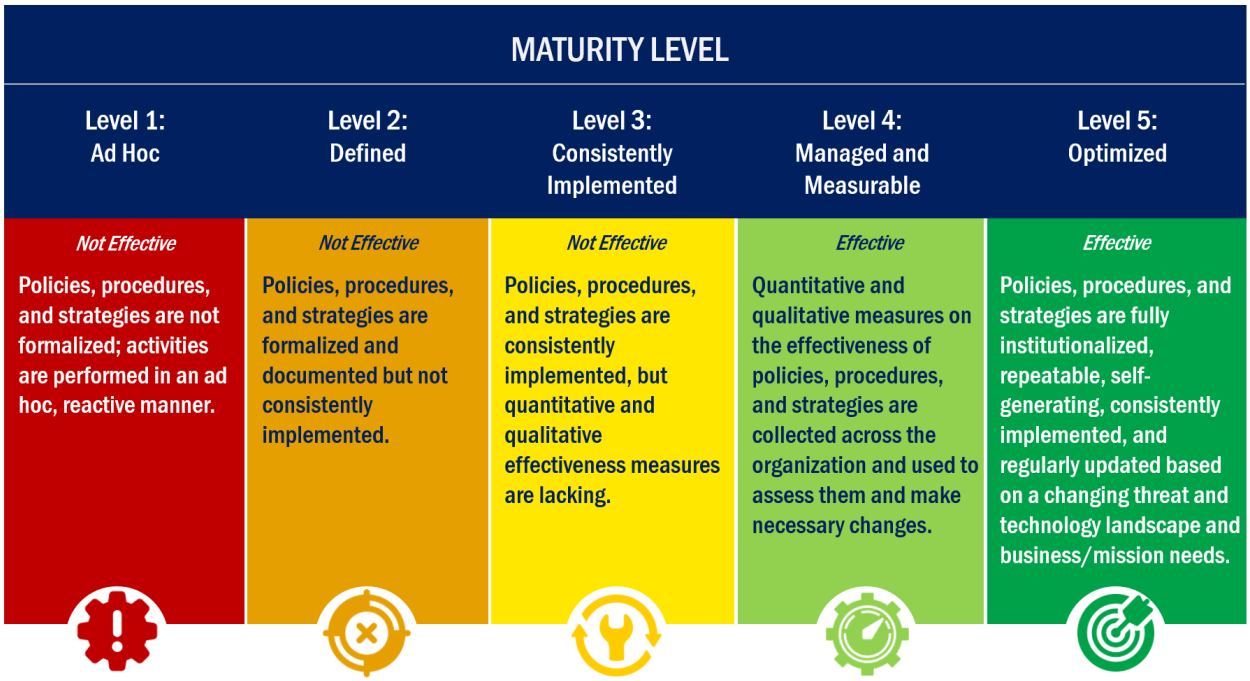
The Inspectors General are required to assess the effectiveness of information security programs based on a maturity model spectrum. Aligning with the Carnegie Mellon Cybersecurity Maturity Model Certification, the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize 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 1 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.

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

[3] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

[4] 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 Responses* (Oct. 8, 2021); and OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).

Figure 1: Inspector General's Assessment Maturity Levels



Source: Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines and Fiscal Year 2021 FISMA Reporting Metrics Version 1.1.

Results of Review

The Cybersecurity Program Was Not Effective in 17 of the 20 Fiscal Year 2022 Core Inspector General Metrics

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.

To determine the effectiveness of the Cybersecurity Program, we evaluated the maturity level of the 20 Core Inspector General Metrics specified in the *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines*. 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 the Government Accountability Office (GAO) audits. These audits, whose results were applicable to the FISMA metrics, were performed, completed,

or contained recommendations that were still open during the evaluation period, July 1, 2021, to May 31, 2022.[5]

The *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* specify that, within the context of the maturity model evaluation process, maturity level 4, *Managed and Measurable*, represents an effective level of security. For the 20 Fiscal Year 2022 Core Inspector General Metrics, we found one metric achieved the *Optimized* maturity level 5 and two metrics achieved the *Managed and Measurable* maturity level 4. However, we determined that six metrics were at a *Consistently Implemented* maturity level 3, and 11 metrics were at a *Defined* maturity level 2. As such, we rated the Cybersecurity Program as "not effective." Figure 2 presents the maturity level ratings for the assessed metrics.

Figure 2: Fiscal Year 2022 Core Inspector General Metrics Assessment Results

Maturity Level	Metric(s)	Count
Level 5: Optimized	55	1
Level 4: Managed and Measurable	54 and 63	2
Level 3: Consistently Implemented	1, 5, 10, 37, 42, and 61	6
Level 2: Defined	2, 3, 14, 20, 21, 30, 31, 32, 36, 47, and 49	11
Level 1: Ad Hoc	None	0

Source: TIGTA's evaluation of the 20 Fiscal Year 2022 Core Inspector General Metrics.

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; maintaining secure configuration settings for its information systems; implementing flaw remediation and patching on a consistent and timely basis; and ensuring that security controls for protecting Personally Identifiable Information are fully implemented.

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.

The detailed results of our evaluation of the maturity level for each of the Fiscal Year 2022 Core Inspector General Metrics are provided below. The metrics are based on Federal Government

[5] The FISMA evaluation period is from July 1, 2021, to June 30, 2022; however, OMB Memorandum M-22-05, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 6, 2021), adjusted the timeline for the Inspector General evaluations of agency effectiveness to align with the budget submission cycle. Due to the early submission cycle, the time frame covered for this review was from July 1, 2021, to May 31, 2022.

guidance and criteria, such as NIST Special Publication 800-53, Revision 5,[6] Executive Order 14028, and OMB memoranda. For metrics rated lower than a maturity level 4, *Managed and Measurable*, we have provided comments to explain our determinations. The effectiveness rating is based on a simple majority, where the most frequent level across the core metrics served as the effective rating. However, we also considered agency-specific factors to determine the final ratings, as instructed by the *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines*.

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 maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections.

   Comments: The IRS cannot always ensure that information systems included in its inventory are subject to the monitoring processes defined within its Information Security Continuous Monitoring (ISCM) Program Plan because of gaps in tools used to monitor its system inventories.

2. To what extent does the organization use standard data elements/taxonomy[7] 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 with the detailed information necessary for tracking and reporting.

   Comments: The IRS has not closed scanning tool gaps necessary to perform checks for unauthorized hardware components/devices and to notify appropriate organizational officials. In addition, several TIGTA audits reported that hardware component inventories were inaccurate and/or incomplete. Also, the IRS has open Plans of Action and Milestones (POA&M) documenting weaknesses in a number of systems due to inaccurate hardware component inventories.

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

[6] NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).

[7] Taxonomy is a scheme of classifications.

mobile applications, utilized in the organization's environment with the detailed information necessary for tracking and reporting.

Comments: The IRS continues to report that it [redacted]

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 organizationally defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization utilizes 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 has not performed all the required privacy risk assessments to provide the necessary input into the organization's enterprise risk management program. However, constructively, the IRS indicated it is incorporating additional Enterprise Risk Profile elements as part of this year's 2022–2023 Enterprise Risk Assessment. For instance, the IRS is in the process of assessing inherent risk for its Enterprise Risk Profile. In addition, this year, it will be explicitly identifying opportunity risks through the enterprise risk assessment process and in the development of the Enterprise Risk Profile. It plans to complete the 2022–2023 Enterprise Risk Profile by the end of Fiscal Year 2022.

10. To what extent does the organization utilize 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 IRS does not perform threat modeling as a normal practice throughout the risk life cycle on applications and systems and when major changes occur in the environment.

Supply Chain Risk Management

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.

    The following components, at a minimum, are defined:

    - The identification and prioritization of externally provided systems, system components, and services as well as how the organization maintains awareness of its upstream suppliers.
    - Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and Supply Chain Risk Management (SCRM) measures for external providers.
    - Tools and techniques to utilize the acquisition process to protect the supply chain, including risk-based processes for evaluating cyber supply chain risks associated with third-party providers, as appropriate.
    - Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.

    Comments: While the IRS has defined and communicated policies and procedures for SCRM, it has not finalized its SCRM Strategy and Implementation plan. However, the IRS indicated it made updates since the last FISMA review, leveraging guidance from the Treasury Department SCRM Program and NIST publications. The SCRM Strategy updates include adding additional detail within the methodology to highlight the planned focus on critical software and High Value Assets, drafting the SCRM risk management process to include risk impact levels and cyber risk categorization, and detailing the multitiered risk management approach (Organizational, Mission/Business, and Information Systems). The IRS will continue to work closely with Treasury Department representatives to establish an IRS-specific supply chain strategy that aligns to the Department's SCRM Program and Strategy.

Configuration Management

20. To what extent does the organization utilize 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: The IRS has open POA&Ms documenting weaknesses in a number of systems due to deficiencies in configuration management, least functionality (e.g., to restrict the use

of software), and vulnerability monitoring and scanning. In addition, the IRS has an open program-level POA&M that documents a deficiency in 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. The IRS has open recommendations in a prior TIGTA report to evaluate and implement controls to provide an age tracking capability for vulnerabilities detected by the configuration compliance scanning tool and update the checklist adjudication process. Furthermore, TIGTA reported that the configuration compliance controls are insufficient.

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?

    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 organizationally defined time frames.
    - 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. [redacted].

Identity, Credential, and Access Management

30. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or an Identity Assurance Level 3/Authenticator Assurance Level 3 credential) for nonprivileged users to access the organization's facilities [organizationally defined entry/exit points], networks, and systems, including for remote access?

    Maturity Level and Corresponding Narrative: ***Defined*** **(Level 2)** – The organization has planned for the use of strong authentication mechanisms for nonprivileged users of the organization's facilities [organizationally defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.

    Comments: According to the IRS, it has not met the requirements outlined in Executive Order 14028 to adopt Multifactor Authentication. [redacted]. According to the IRS, it has implemented Multifactor Authentication mechanisms with Personal Identity Verification for personnel to access the organization's facilities at designated entry/exit points in 52 (16 percent) of the 333 buildings that require Enterprise Physical Access Control Systems. Information

Technology funding for Fiscal Year 2023 through Fiscal Year 2026 is required to complete project plans for the remaining upgrades to the buildings. In addition, the IRS has an open recommendation from a prior GAO report on authentication weaknesses.

31. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or an Identity Assurance Level 3/Authenticator Assurance Level 3 credential) for privileged users to access the organization's facilities [organizationally defined entry/exit points], networks, and systems, including for remote access?

    Maturity Level and Corresponding Narrative: ***Defined*** **(Level 2)** – The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities [organizationally defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.

    Comments: [redacted]. In addition, the IRS has open recommendations in prior TIGTA and GAO reports on authentication weaknesses.

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: ***Defined*** **(Level 2)** – The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.

    Comments: While the IRS has defined its processes for provisioning, managing, and reviewing privileged accounts, the IRS has not consistently implemented controls related to privileged account management. According to the IRS, it is onboarding privileged accounts for new systems and for systems not previously supported by the Total Privileged Access Manager.[8] The IRS indicated that it has increased the number of accounts identified as privileged by 30 percent and implemented enhanced measures for those accounts through its new system. In addition, TIGTA reported that privileged user accounts were not managed as required. Further, the IRS has open recommendations from prior TIGTA and GAO reports on control deficiencies that included unnecessary access rights to privileged accounts. In addition, the IRS has open POA&Ms that document weaknesses in a number of systems due to deficiencies in managing privileged accounts.

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,

[8] Total Privileged Access Manager is the chosen tool for managing elevated access to the Platform in order to meet guidelines from Homeland Security Presidential Directive 12.

throughout the data life cycle (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 specified 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 has not met the requirements outlined in Executive Order 14028. In reference to the Fiscal Year 2022 Chief Information Officer FISMA Monthly Metrics submitted to the OMB on March 15, 2022, the IRS reported that the Data At Rest Encryption Program is using a phased implementation approach for encryption of data at rest and cited technology complexities as the primary barrier for encryption of data in transit. Also, the IRS has open recommendations in a prior TIGTA report on laptop and desktop sanitization practices. In another instance, the IRS has an open recommendation in a prior TIGTA report to ensure that data at rest is encrypted prior to being transferred from the IRS to Private Collection Agencies. [redacted].

37. To what extent has the organization implemented security controls 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 utilizes e-mail authentication technology, audits its Domain Name System records, and ensures the use of valid encryption certificates for its domains.

Comments: The *Fiscal Year 2022 Core Inspector General FISMA Metrics Evaluation Guide* lists OMB Memorandum M-21-07[9] as criteria for this metric. The memorandum requires agencies to develop an Internet Protocol Version 6 Implementation Plan by the end of Fiscal Year 2021. According to the IRS, it has been working towards developing the initial Internet Protocol Version 6 Implementation Plan. In addition, the status of implementing verification tools to detect unauthorized changes to software, firmware, and information is still in progress.

Security Training

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

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

Maturity Level and Corresponding Narrative: *Consistently Implemented* **(Level 3)** – The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and 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 did not provide evidence to support that it uses the output of the workforce skills assessment to provide tailored awareness and specialized security training.

Information Security Continuous Monitoring

47. To what extent does the organization utilize ISCM policies and an ISCM strategy that address 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 an organization-wide strategy. The following areas are included:

- Monitoring requirements at each organizational tier.
- The minimum monitoring frequencies for implemented controls across the organization. The criterion for determining minimum frequencies is 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 defined policies and procedures at each organizational tier. However, it does not support clear visibility of all organizational assets and awareness into vulnerabilities.

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; and 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: Although the IRS has improved the efficiencies of its dashboards and reduced costs, we identified issues with the completeness and accuracy of the System Security Plans.

In addition, according to the IRS, it will fully complete NIST Special Publication 800-53, Revision 5, control assessments by the Fiscal Year 2024 FISMA evaluation period.

Incident Response

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

    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 incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.

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

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

Contingency Planning

61. To what extent does the organization ensure that the results of the 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 result of the BIA are consistently used to determine contingency planning requirements and priorities, including mission-essential functions and high-value assets.

    Comments: According to the IRS, during the last two years, the application inventory requiring a BIA increased significantly. This includes critical applications such as those related to the filing season, mission-essential function hosting applications, and critical infrastructure protection applications. The BIA program prioritized those applications for BIA development, but due to limited resources and the COVID-19 pandemic closures of IRS sites, the business operating divisions had to delay many of their BIA updates to ensure successful completion of the filing season. Therefore, even though we identified some BIAs that were not updated as required, we rated this metric at maturity level 3, *Consistently Implemented*.

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.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS information security program on a maturity model spectrum based on the Fiscal Year 2022 Core Inspector General Metrics. To accomplish our objective, we:

- Determined the maturity level for the core metrics contained in the Fiscal Year 2022 Core Inspector General Metrics that pertain to nine security program components (*i.e.,* domains) and the associated 20 core metrics: Risk Management (five metrics), SCRM (one metric), Configuration Management (two metrics), Identity and Access Management (three metrics), Data Protection and Privacy (two metrics), Security Training (one metric), ISCM (two metrics), Incident Response (two metrics), and Contingency Planning (two metrics).
- Determined the rating for the 20 Fiscal Year 2022 Core Inspector General Metrics by evaluating program documentation and interviewing key subject matter experts. We determined the information security program rating by applying a simple majority rule, whereby the most frequent maturity rating across the metrics served as the effective rating. The *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* 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 of general support systems, major applications, and minor applications with a security classification of moderate or high as the population for this subset. 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 the FISMA metrics that were performed, completed, or contained recommendations that were still open during the Fiscal Year 2022 FISMA evaluation period as well as audit reports from the GAO that contained results applicable to the 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 March through June 2022. This report covers the Fiscal Year 2022 FISMA evaluation period of July 1, 2021, through May 31, 2022.[1] We conducted this evaluation

[1] The FISMA evaluation period is from July 1, 2021, to June 30, 2022; however, OMB Memorandum M-22-05 adjusted the timeline for the Inspectors General evaluation of agency effectiveness to align with the budget submission cycle. Due to the early submission cycle, the time frame covered for this review was from July 1, 2021, to May 31, 2022.

in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our overall objective. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our evaluation objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Joseph Cooney, Audit Manager; Midori Ohno, Lead Auditor; Charles Ekunwe, Senior Auditor; Cari Fogle, Senior Auditor; Steven Stephens, Senior Auditor; and Esther Wilson, Senior Auditor.

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 key IRS subject matter experts, and comparing relevant data and evidence obtained to the *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* provided by the Council of the Inspectors General on Integrity and Efficiency in collaboration with the OMB, the Department of Homeland Security, and Federal Chief Information Officers and Chief Information Security Officers.

Appendix II

Information Technology Security-Related Audits Considered During Our Fiscal Year 2022 Evaluation and the Metric(s) to Which They Apply

1. TIGTA, Report No. 2016-20-050, *Significant Improvements Are Needed to the Mainframe Computing Environment Security* (July 2016) – Metric 32.
2. TIGTA, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020) – Metrics 31 and 32.
3. TIGTA, Report No. 2021-20-003, *Security Controls Over Electronic Crimes Labs Need Improvement* (Dec. 2020) – Metrics 21 and 32.
4. TIGTA, Report No. 2021-20-024, *Improvements Are Needed to More* [redacted] *the Virtual Host Infrastructure Platform* (June 2021) – Metric 21.
5. TIGTA, Report No. 2021-20-056, *Laptop and Desktop Sanitization Practices Need Improvement* (Sept. 2021) – Metrics 3 and 36.
6. TIGTA, Report No. 2021-20-063, [redacted] *Platform Management Needs Improvement* (Sept. 2021) – Metrics 2, 20, 21, and 32.
7. TIGTA, Report No. 2021-20-065, *The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed* (Sept. 2021) – Metric 2.
8. 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.
9. TIGTA, Report No. 2022-20-006, *Vulnerability Scanning and Remediation Processes Need Improvement* (Dec. 2021) – Metric 21.
10. 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 20 and 21.
11. GAO, GAO-18-418, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts* (June 2018) – Metrics 30 and 31.
12. GAO, GAO-19-473RUS, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019) – Metric 3.
13. GAO, GAO-22-105558SU, *Management Report: IRS Needs to Improve Financial Reporting and Information System Controls* (May 2022) – Metrics 32 and 36.

Appendix III

Abbreviations

BIA	Business Impact Analysis
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
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,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

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