

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation

September 28, 2021

Report Number: 2021-20-072

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

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.

Impact on Taxpayers

FISMA focuses on improving oversight of Federal information security programs and facilitating the progress in correcting agency information security weaknesses. In Fiscal Year 2020, the IRS received and processed more than 240 million Federal tax returns and supplemental documents, which represent 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 2021, 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 levels for five function areas: IDENTIFY (organizational understanding to manage cybersecurity risk to assets and capabilities), PROTECT (appropriate safeguards to ensure delivery of critical services), DETECT (appropriate activities to identify the occurrence of a cybersecurity event), RESPOND (appropriate activities to take action regarding a detected cybersecurity event), and RECOVER (appropriate activities to restore capabilities or services that are impaired due to a cybersecurity event).

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. However, due to program components that were not at an acceptable maturity level, the Cybersecurity Program was not fully effective. The Department of Homeland Security's scoring methodology defines "effective" as being at a maturity level 4, *Managed and Measurable*, or above.

Based on these evaluation parameters, TIGTA rated three Cybersecurity Framework function areas (PROTECT, RESPOND and RECOVER) as "effective" and two function areas (IDENTIFY and DETECT) as "not effective."

The IDENTIFY function area, which was based on the Risk Management metrics, and the DETECT function area, which was based on the Information Security Continuous Monitoring metrics, were rated at the maturity level 2, *Defined*.

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

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program components 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.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2021

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

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Fiscal Year 2021 IRS Federal Information Security
Modernization Act Evaluation (Audit # 202120001)

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 2021. 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 Department of Homeland Security. Our overall objective was to assess the effectiveness of the IRS information security program on a maturity model spectrum. This audit is included in our Fiscal Year 2021 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 Effective in Three of the Five Cybersecurity Framework Function Areas	Page 3
---	--------

Appendices

Appendix I – Detailed Objective, Scope, and Methodology	Page 32
---	---------

Appendix II – Information Technology Security-Related Audits Considered During Our Fiscal Year 2021 Evaluation and the Metric(s) to Which They Apply	Page 34
--	---------

Appendix III – Abbreviations	Page 36
--	---------

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 the 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 (DHS), 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 Department of the Treasury 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 2020, the IRS collected close to \$3.5 trillion in gross taxes and processed more than 240 million Federal tax returns and supplemental documents, which represent 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's systems and its data.

Fiscal Year 2021 Inspector General FISMA Reporting Requirements

The Fiscal Year 2021 Inspector General FISMA Reporting Metrics, developed as a collaborative effort among the OMB, the DHS, and the Council of the Inspectors General on Integrity and Efficiency, align with the five cybersecurity function areas in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, hereafter referred to as the Cybersecurity Framework.²

Figure 1 presents the five Cybersecurity Framework function areas and aligns each with the associated security program component(s) (or metric domain(s)).

Figure 1: Alignment of the NIST Cybersecurity Framework Function Areas to the Fiscal Year 2021 Inspector General FISMA Metric Domains

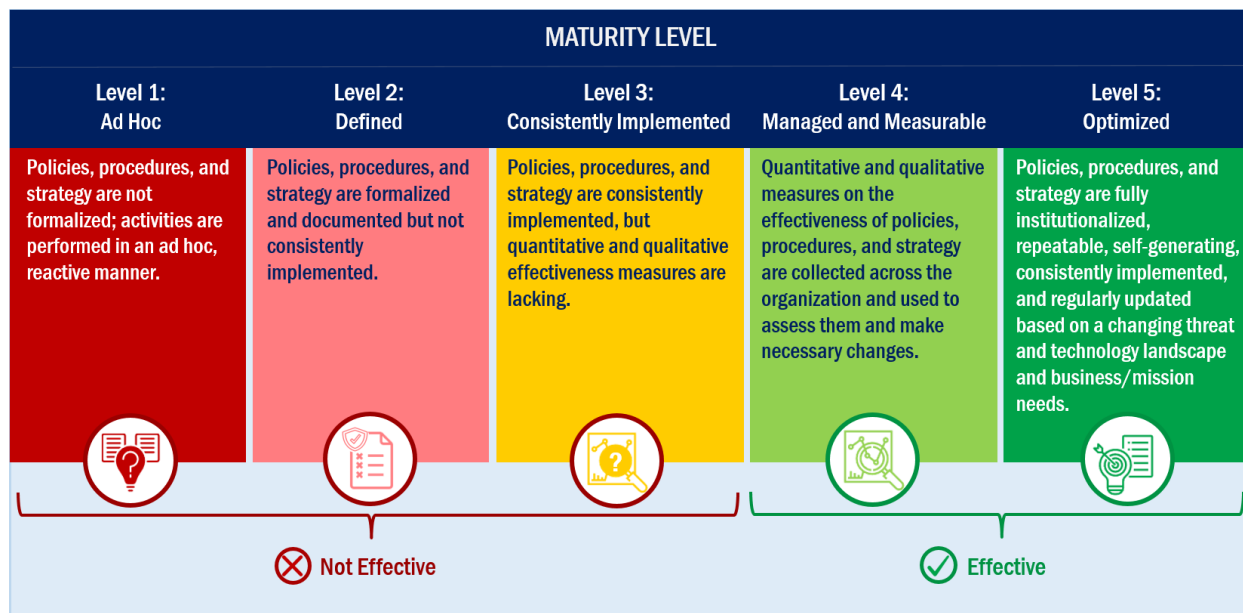
 IDENTIFY	 PROTECT	 DETECT	 RESPOND	 RECOVER
Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Develop and implement the appropriate activities to identify 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 Year 2021 Inspector General FISMA Metric Domains				
 Risk Management  Supply Chain Risk Management (SCRM)	 Configuration Management  Identity and Access Management  Data Protection and Privacy  Security Training	 Information Security Continuous Monitoring (ISCM)	 Incident Response	 Contingency Planning

Source: *Fiscal Year 2021 Inspector General FISMA Reporting Metrics and NIST Framework for Improving Critical Infrastructure Cybersecurity*.

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum in which the metric domains 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.

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

Figure 2: Inspector General’s Assessment Maturity Levels



Source: Fiscal Year 2021 Inspector General FISMA Reporting Metrics.

Results of Review

The Cybersecurity Program Was Effective in Three of the Five Cybersecurity Framework Function Areas

The IRS established a Cybersecurity Program that 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 program metrics specified by the DHS in the Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1 (May 12, 2021). 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 FISMA evaluation period, July 1, 2020, to June 30, 2021. See Appendix II for a list of these audits with notations as to which metric(s) the reports applied. As shown in Figure 3, TIGTA rated three Cybersecurity Framework function areas as “effective” and two as “not effective.”

Figure 3: Maturity Levels by Function Area

Overall Effectiveness of Each Function Area				
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Level 2: Defined <i>Not Effective</i>	Level 4: Managed and Measurable <i>Effective</i>	Level 2: Defined <i>Not Effective</i>	Level 4: Managed and Measurable <i>Effective</i>	Level 4: Managed and Measurable <i>Effective</i>
Assessed Maturity Levels for Fiscal Year 2021 Inspector General FISMA Metric Domains				
Risk Management Level 2: Defined	Configuration Management Level 2: Defined	ISCM Level 2: Defined	Incident Response Level 4: Managed and Measurable	Contingency Planning Level 4: Managed and Measurable
SCRM ¹ Level 1: Ad Hoc	Identity and Access Management Level 3: Consistently Implemented			
	Data Protection and Privacy Level 4: Managed and Measurable			
	Security Training Level 4: Managed and Measurable			

¹ The SCRM metric was not included in the overall rating for the *Identify* function rating.

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

The Cybersecurity Framework function areas of PROTECT, RESPOND, and RECOVER were rated at a *Managed and Measurable* maturity level

The Fiscal Year 2021 Inspector General FISMA Reporting Metrics 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 five Cybersecurity Framework function areas, we found that two function areas, RESPOND and RECOVER, and their respective security program components, Incident Response and Contingency Planning, achieved the *Managed and Measurable* maturity level 4 and were deemed as "effective" in accordance with the Fiscal Year 2021 Inspector General FISMA Reporting Metrics. Details of the results of our evaluation of these maturity levels are presented on pages 27 and 29, respectively.

The PROTECT function area consists of four security program components: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. Based on the Fiscal Year 2021 Inspector General FISMA Reporting Metrics, we found that the performance metrics for Data Protection and Privacy and for Security Training achieved a *Managed and Measurable* maturity level 4, and we therefore considered them "effective." However, we determined that the Identity and Access Management security program component was at a *Consistently Implemented* maturity level 3 and the Configuration Management security program component was at a *Defined* maturity level 2. As such, we considered these program components "not effective." The overall maturity level for the PROTECT function area is at a *Managed and Measurable* maturity level 4 in accordance with the

Fiscal Year 2021 Inspector General FISMA Reporting Metrics. As a result, we consider the function area “effective.” Details of the results of our evaluation of these maturity levels are presented on pages 15, 18, 21, and 23, respectively.

While the PROTECT function area is at an effective level, the following examples are Configuration Management metrics that did not meet the Managed and Measurable maturity level 4.

- Metric 19 pertains to utilizing baseline configurations for information systems. While the IRS has defined baseline configurations, it has not ensured that its information systems consistently maintain the baseline or component inventories in compliance with IRS policy.
- Metric 21 pertains to managing software vulnerabilities through flaw remediation processes, including patch management. While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis.

The Cybersecurity Framework function areas of IDENTIFY and DETECT were rated at a *Defined* maturity level

Based on the Fiscal Year 2021 Inspector General FISMA Reporting Metrics, we found that the IDENTIFY and DETECT function areas and their respective security program components, Risk Management and ISCM, met a Defined maturity level 2, which we considered “not effective.” Details of our evaluation are presented on pages 7 and 25, respectively. The following examples are metrics that did not meet the Managed and Measurable maturity level 4.

- Metric 1 pertains to maintaining a comprehensive and accurate inventory of its information systems. Both the IRS and TIGTA have identified weaknesses in the ability to maintain a comprehensive and accurate inventory of its information systems. In addition, the IRS’s FISMA system inventory and security artifact repository, Treasury FISMA Inventory Management System (TFIMS), had inaccurate inventory on cloud systems.
- Metrics 2 and 3 pertain to tracking and reporting on an up-to-date inventory of hardware and software assets, respectively. The IRS has not implemented the Continuous Diagnostics and Mitigation (CDM) Phase 1 scanning tool necessary to perform checks for unauthorized hardware components/devices and software, and to notify appropriate organizational officials. In addition, the IRS has open Plan of Action and Milestones (POA&M) which documents weaknesses in a number of systems due to inaccurate hardware/software component inventories.
- Metric 47 pertains to the ISCM strategy that addresses ISCM requirements and activities at each organizational tier. The IRS has developed the ISCM strategy, but it has not fully developed tools that support an accurate inventory.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA requirements, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

Under the Identify function area, the Fiscal Year 2021 Inspector General FISMA metrics introduced a new metric domain on SCRM

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. One such area is increasing the maturity of the Federal government's SCRM practices. As noted in the Federal Acquisition Supply Chain Security Act of 2018,³ agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks.

The SCRM domain, introduced in this year within the Identify function, consists of five metrics, one of which is a summary rating of the previous four metrics. These four metrics cover utilizing a supply chain management strategy; policies and procedures; actions to ensure products, systems, system components, and services with external providers are consistent with requirements; and actions to ensure that counterfeit components are detected and prevented from entering the organization's systems.

We rated all four metrics at an *Ad Hoc* maturity level 1. For example, the IRS developed a draft SCRM strategy that provides high-level strategic objectives, but the strategy was missing key elements such as agency risk tolerance and the risk assessment process. The IRS indicated that its SCRM program is in the beginning stages of establishing policies, procedures, and standards for vendors. These new metrics were not considered in the maturity rating for the Identify function area to provide agencies with sufficient time to fully implement these new requirements and standards.

TIGTA's evaluation of the Fiscal Year 2021 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the Fiscal Year 2021 Inspector General FISMA Reporting Metrics are provided below. The metrics are based on Federal Government guidance and criteria, such as NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013),⁴ and OMB memoranda. For metrics we rated lower than a maturity level 4, Managed and Measurable, we have provided comments to explain the reasons why. The overall function area rating is based on a simple majority of all performance metrics. However, we also considered agency-specific factors to determine the final ratings, as instructed by the Fiscal Year 2021 Inspector General FISMA Reporting Metrics.

³ Title II of Public Law No. 115-390 (December 2018).

⁴ Revision 4 of this Special Publication was the primary criteria cited in the Fiscal Year 2021 FISMA Reporting Metrics, with the exception for the SCRM area. The NIST updated this Special Publication to Revision 5, published in September 2020 and includes updates as of December 10, 2020.

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: **Defined (Level 2)** – The organization has defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.

Comments: Both the IRS and TIGTA identified weaknesses in the IRS's ability to maintain a comprehensive and accurate inventory of its information systems. The IRS reported that it does not currently have a tool that can detect the presence of unauthorized hardware, software, and firmware components and notify appropriate organizational officials. The IRS has identified a number of weaknesses with Knowledge Incident/Problem Service Asset Management, its official inventory repository, reflecting an inaccurate inventory. TIGTA reviews identified issues with the IRS inventory processes. For instance, TIGTA found the official inventory did not reconcile with the Information System Contingency Plan, production server information was missing required data elements, and nine servers in the testing or development environment were misclassified as production servers. In addition, TIGTA reported there is no information system component inventory for a web application. Also, the IRS has an open recommendation in a prior TIGTA report to ensure that all systems are included in the As-Built Architecture⁵ with complete and accurate information, including the managing organization(s), application age, and programming language. According to the IRS, it has made progress with the implementation of CDM scanning tools to identify devices connected to the network and to correlate their FISMA boundary designation and authorization to be connected to the network. However, gaps remain due to the size, complexity, and variety of platforms the IRS operates.

In addition, the IRS manages various inventories primarily with spreadsheets. Managing inventory with spreadsheets is based on a manual process, which creates gaps, can be error-prone, and is time and labor intensive. For example, the IRS's FISMA system inventory and security artifact repository, TFIMS, does not include all cloud systems and contained cloud systems no longer on the June 2021 Enterprise Cloud Inventory Report. Overall, we found inconsistencies in cloud systems reported in the TFIMS, the As-Built Architecture, and the Enterprise Cloud Inventory. We also found the number of public-facing applications and websites listed on a spreadsheet inconsistent with the IRS monthly reporting to the Department of the Treasury. Further, the spreadsheet did not contain a comprehensive listing of web applications.

2. To what extent does the organization use standard data elements/taxonomy⁶ to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished

 Risk Management	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	0
Level 3: Consistently Implemented	4
Level 2: Defined	6 
Level 1: Ad Hoc	0

⁵ The IRS Enterprise Architecture As-Built Architecture presents an enterprise view of the IRS's current information technology and business environments.

⁶ Taxonomy is a scheme of classifications.

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 implemented CDM Phase 1 scanning tool gaps necessary to perform checks for unauthorized hardware components/devices and to notify appropriate organizational officials. [REDACTED]

[REDACTED]. Lastly, the IRS has open POA&Ms documenting weaknesses in a number of systems due to inaccurate hardware component inventories. According to the IRS, it has made progress with the implementation of CDM scanning tools to identify devices connected to the network and to correlate their FISMA boundary designation and authorization to be connected to the network. However, gaps remain due to the size, complexity, and variety of platforms the IRS operates.

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

Comments: We found CDM Phase 1 implementation gaps in the IRS's enterprise solution for software asset and configuration management. In addition, the IRS continues to report that it does not currently have a tool that can detect the presence of unauthorized hardware, software, and firmware components and notify appropriate organizational officials.

Further, TIGTA reported that the Endpoint Detection and Response solution was neither fully accounted for nor deployed to all required workstations enterprise-wide. In another instance, [REDACTED]

[REDACTED]. In addition, the IRS has an open recommendation in a prior TIGTA report to create and execute a plan to periodically monitor and compare software running on the enterprise against the Enterprise Architecture Enterprise Standard Profile⁷ Product Catalog for accuracy. Lastly, the IRS has open POA&Ms documenting weaknesses in a number of systems due to inaccurate software inventories. According to the IRS, it has made progress with the implementation of CDM scanning tools to identify devices connected to the network and to correlate their FISMA boundary designation and authorization to be connected to the network. However, gaps remain due to the size, complexity, and variety of platforms the IRS operates.

⁷ The authoritative repository for IRS-approved products and standards.

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: **Consistently Implemented (Level 3)** – The organization consistently implements its policies, procedures, and processes for system categorization, review, and communication, including for high-value assets, as appropriate. Security categorizations consider potential adverse impacts to organization operations, organizational assets, individuals, other organizations, and the Nation. System categorization levels are used to guide risk management decisions, such as the allocation, selection, and implementation of appropriate control baselines.

Comments: The IRS did not timely complete or update the Business Impact Analysis (BIA) as required by its policy for six of the seven information systems selected for the Fiscal Year 2021 FISMA review. The IRS policy requires a BIA to be completed prior to Authorization to Operate, or if already granted an Authorization to Operate with the next update of the system's contingency plan. According to the IRS, business operating divisions have filing season competing priorities, especially where interdependencies (applications feeding data to the primary application or the primary application feeding upstream applications) can cause the schedule to slip by a few months. Most of the BIAs are updated in a timely manner. For those rare instances where the schedule can slip, they accommodate the primary role of the business operating division to support their taxpayer responsibilities first. For the future, they will update their schedule to allow for more lead time to accommodate for this issue.

However, the Fiscal Year 2021 Inspector General FISMA Reporting Metrics allow for some discretion on maturity level rating, we rated this program area at maturity level 3, *Consistently Implemented*, despite deficiencies that adversely impact this metric as noted in Metric 11.

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: **Defined (Level 2)** – The organization has defined and communicated the policies, procedures, and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components: risk framing, risk assessment, risk response, and risk monitoring.

Comments: The IRS developed the 2020/2021 IRS Enterprise Risk Profile and 2019/2020 Fraud Risk Profile. The IRS stated that both profiles were developed and approved by the agency's "Risk Management Council," which is the IRS Executive Risk Committee. However, the risk profiles are missing key elements as required by OMB⁸ Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. In addition, the IRS has an open GAO recommendation related to its Fraud Risk Profile. The

⁸ OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016).

GAO reported that the IRS did not conduct an adequate assessment of risks and controls of an external system. Further, the IRS has an open recommendation for not implementing a fully integrated ISCM process that includes privacy risks. The IRS closed this recommendation after the Fiscal Year 2021 FISMA review period.

6. To what extent does the organization utilize 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: **Defined (Level 2)** – The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. In addition, the organization has defined how it implements system security engineering principles and software assurance processes for mobile applications, within its System Development Life Cycle.⁹

Comments: The IRS has not implemented controls to protect against supply chain threats to the information system, system component, or information system service by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.¹⁰ In addition, the IRS has not finalized its SCRM strategy and implementation plan, policies, and processes to guide and govern SCRM activities. Further, TIGTA reported the Data at Rest Encryption project did not follow the Enterprise Life Cycle requirements that include developing a Business System Report prior to starting development work. In addition, TIGTA identified that the IRS did not update significant Enterprise Life Cycle artifacts as required and the Data at Rest Encryption Business System Report was not completed and approved. In another TIGTA report, the Endpoint Detection and Response solution was not at full operating capability on all enterprise workstations as reported by the IRS. Further, the IRS has open recommendations from prior TIGTA reports for the IRS to create and execute a plan to periodically monitor and compare software running on the enterprise against the Enterprise Architecture Enterprise Standard Profile Product Catalog for accuracy, and to remove unauthorized software or update the Enterprise Standard Profile Product Catalog to reflect the correct information, if warranted.

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

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

⁹ System Development Life Cycle is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.

¹⁰ The Supply Chain Protection (SA-12) control is required by NIST Special Publication 800-53, revision 4. The IRS indicated that the Department of the Treasury is responsible for implementing this control. However, the Department of the Treasury is responsible for implementing the Supply Chain Protection – Use of All-Source Intelligence (SA 12(8)) control portion of the SCRM process.

Comments: Based on the performance results for metrics 1 through 6, this function was evaluated at maturity level 2, *Defined*. However, the Fiscal Year 2021 Inspector General FISMA Reporting Metrics allow for some discretion on maturity level ratings, and we believe the IRS is making progress in transitioning to individuals performing the cybersecurity risk management roles and responsibilities as defined, including roles and responsibilities related to integration with enterprise risk management processes. We based our assessment on our review of risk charters, committees' meeting minutes, and other artifacts that show sufficient Information Technology, Cybersecurity governance, and integration with enterprise risk management processes (see Metric 11). As such, we rated this program area at maturity level 3, *Consistently Implemented*.

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

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

Comments: We selected open TIGTA security recommendations identified in the Joint Audit Management Enterprise System during Calendar Years 2019 through 2020 to determine whether the IRS was creating POA&Ms for security weaknesses within 30 days as required. Out of 35 security-related weaknesses, 27 did not have POA&Ms created in TFIMS. After June 30, 2021, the IRS created 14 POA&Ms. Ten of these 14 POA&Ms were created after we brought this to the IRS's attention. The IRS was not fully aware of its responsibilities to create POA&Ms for TIGTA security recommendations. In addition, the IRS did not timely create POA&Ms for weaknesses identified in two Cloud Security Assessment Reports. The IRS's Enterprise FISMA Services office did not timely receive the Cloud Security Assessment Reports; therefore, it notified the system owners after these reports were received to create POA&Ms.

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

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

Comments: The IRS utilizes a cybersecurity risk register to ensure that information about risks is communicated in a timely and effective manner to appropriate internal and external stakeholders with a need-to-know. In reference to Metric 49, System Security Plans did not always meet quality standards. For example, we found System Security Plans with information that was not appropriate, current, complete, accurate, accessible, and as such, not timely. Without quality information, management's (including internal and external stakeholders) ability to make informed decisions and evaluate the entity's performance in

achieving key objectives and addressing risks is limited. However, the Fiscal Year 2021 Inspector General FISMA Reporting Metrics allow for some discretion on maturity level ratings, and based on significant improvement discussed in metric 11, we rated this program area at maturity level 3, *Consistently Implemented*.

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: While the IRS has performed a threat modeling assessment, the information provided did not support threat modeling as a normal practice throughout the risk life cycle on applications and systems, and when major changes occur in the environment.

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. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Overall Risk Management Maturity Level: ***Defined (Level 2)*** – Based on the performance results for metrics 1 through 10, this function was evaluated as maturity level 2, *Defined*.

Overall Risk Management Program Comments: The IRS's risk management program is not effective because it did not meet the *Managed and Measurable* maturity level 4. However, we acknowledge improvements in the IRS Information Technology Risk Management Program that are listed below and weighted in our decision to elevate specific metric ratings in reference to metrics 7 and 9. The Information Technology Risk Management Program improvements included the following accomplishments:

- Major efforts to continue filling gaps in CDM Phase 1 Security Configuration Setting Management Scanning to identify cybersecurity risks on an ongoing basis.
- Developing the Information Technology Risk Management Program Plan that includes the Governance and Operating Models, program roles and responsibilities, and the Information Technology-wide risk management process. In addition, it addresses the interactions between the Information Technology Risk Management Plan and the enterprise risk management strategies and processes of the Office of the Chief Risk Officer.
- Continued progress to establish Associate Chief Information Officer Risk Review Boards and Information Technology Risk Advocates/Liaisons processes.
- In 2020, the Cybersecurity function began utilizing its own Cyber Risk Register and Dashboard that focuses directly on managing security risks, along with the Item Tracking Reporting and Control system used for risk management and tracking enterprise-wide.

- In January 2020, the Cybersecurity Enterprise FISMA Services office automated the Risk-Based Decision (RBD) process with implementing the Online RBD application that documents and accepts risks within the IRS environment; provides automated notifications and tracking; and has interactive capabilities for review and accuracy of the RBDs. The IRS also made improvements on establishing RBD dashboards, training employees, linking devices to the RBDs to one of its CDM Phase 1 near-real time analytics tools, and establishing management and customer reports.

Despite these improvements, the Risk Management Program metric ratings were adversely impacted by the following deficiencies:

- CDM Configuration Setting Management Capability Scanning Gaps in reference to metrics 1, 2, and 3.
- SCRM requirements must be considered in metrics 4, 6, 7, and 9.
- Cyber Security Assessment Management System Security Plans accuracy in reference to metrics 6 and 9.
- High-value assets categorization/assessment/prioritization in reference to metrics 4, 7, and 9.

IDENTIFY Function Area – Supply Chain Risk Management

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



Maturity Level and Corresponding Narrative: **Ad Hoc (Level 1)** – The organization has not defined and communicated an organization-wide SCRM strategy.

Comments: The IRS has developed a draft SCRM strategy document that provides high-level draft strategic objectives; however, it is missing key elements for addressing SCRM. For example, the draft SCRM strategy does not explicitly provide the agency's risk tolerance in clear and unambiguous terms. In addition, the risk assessment process is not fully defined. The risk assessment process is dependent on having a proper and updated asset inventory. The IRS struggles to maintain accurate, complete, and updated asset inventories, as noted in metrics 2 and 19. The IRS indicates it will update and refine its strategy as it receives additional guidance from the Treasury SCRM program.

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

Maturity Level and Corresponding Narrative: **Ad Hoc (Level 1)** – The organization has not defined and communicated its SCRM policies, procedures, and processes.

Comments: The IRS SCRM program is in the beginning stages of establishing policies, procedures, and standards for vendors. The IRS has developed a draft SCRM strategy

 Supply Chain Risk Management	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	0
Level 3: Consistently Implemented	0
Level 2: Defined	0
Level 1: Ad Hoc	4 

document that provides high-level draft strategic objectives; however it is missing key elements for addressing SCRM. For example, the draft SCRM strategy does not explicitly provide the agency's risk tolerance in clear and unambiguous terms. In addition, the risk assessment process is not fully defined. The risk assessment process is dependent on having a proper and updated asset inventory. The IRS struggles to maintain accurate, complete, and updated asset inventories, as noted in metrics 2 and 19. The IRS indicated that the Cybersecurity function is evaluating the updated NIST Special Publication 800-53, Revision 5 guidance and plans to integrate the supply chain-related security controls, enhancements, and objectives into security assessments and the continuous monitoring methodology as applicable in Fiscal Year 2022.

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?

Maturity Level and Corresponding Narrative: **Ad Hoc (Level 1)** – The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and SCRM requirements.

Comments: The IRS indicated that its SCRM program is in the beginning stages of establishing policies, procedures, and standards for vendors. IRS current policies, procedures, and processes do not address SCRM requirements in NIST Special Publication 800-53, Revision 5. The IRS indicated that the Cybersecurity function is evaluating the NIST Special Publication 800-53, Revision 5 guidance and plans to integrate the supply chain-related security controls, enhancements, and objectives into security assessments and the continuous monitoring methodology as applicable in Fiscal Year 2022.

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: **Ad Hoc (Level 1)** – The organization has not defined and communicated its component authenticity policies and procedures.

Comments: The IRS indicated that its SCRM program is in the beginning stages of establishing policies, procedures, and standards for vendors, and it has not defined component authenticity policies and procedures. In partnership with the Department of the Treasury, it has begun developing a variety of problem statements with draft contractual language with references to NIST Special Publication 800-53 Revision 5 controls. This contractual language is an initial draft and has not been reviewed, approved, or incorporated into any contracts.

16. Provide any additional information on the effectiveness (positive or negative) of the organization's SCRM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Overall SCRM Maturity Level: **Ad Hoc (Level 1)** – Based on the performance results for metrics 12 through 15, this function was evaluated at maturity level 1, *Ad Hoc*.

Overall SCRM Program Comments: The IRS's SCRM program is not effective because it did not meet the *Managed and Measurable* maturity level 4. We did not include the results in the overall ratings for the IDENTIFY function rating.



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) – Individuals are performing the roles and responsibilities that have been defined across the organization.

Comments: The IRS did not specifically address allocation of resources (people, processes, and technology) in a risk-based manner and in addition did not address accountability for carrying out roles and responsibilities effectively.

 Configuration Management	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	1
Level 3: Consistently Implemented	2
Level 2: Defined	5 
Level 1: Ad Hoc	0

18. To what extent does the organization utilize 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: **Managed and Measurable (Level 4)** – The organization monitors, analyzes, and reports to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, uses this information to take corrective actions when necessary, and ensures that data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

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

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

Comments: The IRS has not fully defined baseline configurations, nor has it ensured that its information systems consistently maintain the baseline or component inventories. The IRS has several open POA&Ms referencing weaknesses in not maintaining configuration baselines.

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 cannot fully ensure the principle of least functionality. The current network implementation does not adequately segment and segregate the high-value asset from the rest of the IRS's systems and users. In addition, as indicated in the IRS's self-assessment, as part of the CDM program, it is awaiting the selection, implementation, and configuration of a software tool by the DHS that has software assessing capabilities to ensure that only authorized software programs are implemented on the network. Further, based on the *Defined* maturity level of metrics 1 through 3, the IRS has not collectively met the Consistently Implemented maturity level 3 for this metric.

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 organizational-defined time frames, and incorporating flaw remediation into the organization's configuration management processes.

Comments: While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis. [REDACTED]

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

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization consistently implements TIC requirements based on OMB M-19-26.¹¹ This includes consistent implementation of defined TIC security controls, as appropriate, and ensuring that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. The agency develops and maintains an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.

Comments: The IRS has fully implemented the Common Communication Gateway, which is the IRS's DHS-approved TIC up to version 2.0. According to the IRS, there are no identified and approved use cases for the TIC 3.0. Until the TIC 3.0 standard is finalized and the IRS receives direction from the Department of the Treasury, it will continue with the traditional use case and TIC 2.0 implementation.

¹¹ OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative* (Sept. 2019).

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 Configuration Control Board,¹² 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: While the IRS has defined policy and procedures for managing configuration change control, these policies and procedures have not been consistently followed at the information system level. The IRS has multiple open POA&Ms referencing weaknesses in configuration change controls.

24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for Internet-accessible Federal systems?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has developed, documented, and publicly disseminated a comprehensive VDP. The following elements are addressed: the systems in scope, types of testing allowed, reporting mechanisms, timely feedback, and remediation. In addition, the organization has updated its vulnerability disclosure handling procedures to support the implementation of its VDP.

Comments: The Department of the Treasury is responsible for the VDP program and we confirmed with the Treasury Office of Inspector General contractor that the Department of the Treasury is working on its VDP. When the VDP has been completed and guidance is provided to the bureaus, the IRS will be responsible for implementing it on its Internet-accessible systems.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

Overall Configuration Management Maturity Level: **Defined (Level 2)** – Based on the performance results for metrics 17 through 24, this function was evaluated at maturity level 2, *Defined*.

Overall Configuration Management Comments: The IRS's configuration management program is not effective because it did not meet the *Managed and Measurable* maturity level 4.

¹² The Configuration Control Board is a group of qualified people with responsibilities for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational lifestyle of an information system.

PROTECT Function Area – Identity and Access Management

26. To what extent have the roles and responsibilities of Identity, Credential, and Access Management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

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

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

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has developed a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities. The organization has developed milestones for how it plans to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17,¹³ and Phase 2 of the DHS's CDM program, as appropriate.

Comments: While the IRS is following the Treasury Enterprise Identity, Credential, and Access Management roadmap and business case to guide its efforts, the CDM Phase 2 schedule shows that the IRS is behind schedule.



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: **Managed and Measurable (Level 4)** – The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties.

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

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

30. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or an Identity Assurance Level 3/Authenticator Assurance

 Identity & Access Management	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	3
Level 3: Consistently Implemented	0 
Level 2: Defined	5
Level 1: Ad Hoc	0

¹³ OMB M-19-17, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management* (May 2019).

Level 3 credential) 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: **Defined (Level 2)** – The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.

Comments: While the IRS reported 92 percent of its non-privileged users are required to use Personal Identity Verification cards to access the network, it also reported that only 80 (59 percent) of 136 internal systems are configured to require Personal Identity Verification cards. The IRS has open POA&Ms on not implementing multifactor authentication on its applications. An external review conducted by the [REDACTED]¹⁴. In addition, the IRS has open recommendations in prior TIGTA reports on authentication weaknesses. Further, the GAO reported authentication weaknesses. According to the IRS, it is in the planning phase to implement a tool to mitigate the 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 [organization-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 [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.

Comments: While the IRS reported 100 percent of its privileged users are required to use Personal Identity Verification cards to access the network, it reported that only 80 (59 percent) of 136 internal systems are configured to require Personal Identification Verification cards. [REDACTED]

[REDACTED]. Further, the IRS has an open recommendation on prior TIGTA and GAO reports on authentication weaknesses. According to the IRS, it is in the process of deploying a tool to mitigate the weaknesses by the end of Fiscal Year 2022.

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. [REDACTED]

[REDACTED]. In addition, the IRS has open recommendations from prior TIGTA reports on inconsistent monitoring of systems and accounts, and not limiting the duration that privileged accounts can be logged in.

33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?

Maturity Level and Corresponding Narrative: **Defined (Level 2)** – The organization has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.

Comments: The IRS has not fully implemented encryption solutions that are compliant with Federal Information Processing Standard Publication 140-2¹⁵ on all of its remote access connections. TIGTA and the GAO reported issues with inadequate encryption to protect systems and data.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Overall Identity and Access Management Maturity Level: **Consistently Implemented (Level 3)** – Based on the performance results for metrics 26 through 33, this function was evaluated at maturity level 2, *Defined*. However, the Fiscal Year 2021 Inspector General FISMA Reporting Metrics allow for some discretion on maturity level ratings, and we believe the IRS is making significant progress in transitioning to the more secure Identity, Credential, and Access Management targeted state. As such, we rated this program area at maturity level 3, *Consistently Implemented*.

Overall Identity and Access Management Program Comments: The IRS's identity and access management program is not effective because it did not meet the *Managed and Measurable* maturity level 4.

¹⁵ NIST, Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules* (May 2001).

PROTECT Function Area – Data Protection and Privacy

35. To what extent has the organization developed a privacy program for the protection of Personally Identifiable Information (PII) that is collected, used, maintained, shared, and disposed of by information systems?

Maturity Level and Corresponding Narrative: **Defined**

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

Comments: The IRS has implemented its privacy program by dedicating resources and conducting privacy impact assessments and system of records notices. However, we could not verify whether the inventory of the collection and use of PII that the IRS maintains is accurate and complete. While it does maintain a system for tracking this information, based on TIGTA audit findings, there is limited assurance that it includes information from all systems containing PII. Specifically, TIGTA reported that the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and PII.

36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, 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 organization's policies and procedures have been defined and communicated for the specified areas, it has not ensured that they are consistently implemented. In addition, TIGTA reported that the task of encrypting sensitive data across the entire IRS enterprise presents significant challenges. Further, TIGTA reported that the IRS is not using an approved sanitization product to overwrite sensitive taxpayer data on laptop and desktop hard disks, nor is it annually testing its sanitization equipment and procedures at the Memphis Sanitization Site to verify that the intended sanitization results are being achieved. In addition, while the IRS is sanitizing most of its laptops and desktops, its process to independently verify the sanitization of each laptop and desktop is ineffective.

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

 Data Protection & Privacy	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	2 
Level 3: Consistently Implemented	1
Level 2: Defined	2
Level 1: Ad Hoc	0

traffic passes through a web content filter that protects against phishing, 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 PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes e-mail authentication technology and ensures the use of valid encryption certificates for its domains.

Comments: The IRS did not provide sufficient evidence to support that it analyzes qualitative and quantitative measures on the performance of and that it conducts exfiltration exercises for its enhanced network defenses (*i.e.*, dashboards to show that the IRS is measuring performance of the defenses).

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: ***Managed and Measurable (Level 4)*** - The organization measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

Overall Data Protection and Privacy Maturity Level: ***Managed and Measurable (Level 4)*** – Based on the performance results for metrics 35 through 39, this function was evaluated at maturity level 4, *Managed and Measurable*.

Overall Data Protection and Privacy Comments: The IRS's data protection and privacy program is effective because it meets the *Managed and Measurable* maturity level 4.

PROTECT Function Area – Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization-wide security awareness and training program as well as the awareness and training-related roles and responsibilities of system users and those with significant security responsibilities.)

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

 Security Training	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	3 
Level 3: Consistently Implemented	1
Level 2: Defined	1
Level 1: Ad Hoc	0

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?

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 has made progress in addressing knowledge, skills, and abilities gaps identified through its workforce assessment.

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as e-mail advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools), frequency of training, and deployment methods.)

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 security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

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? (Note: awareness training topics should include, as appropriate:

consideration of organizational policies, roles, and responsibilities; secure e-mail, browsing, and remote access practices; mobile device security; secure use of social media; phishing; malware; physical security; and security incident reporting?

Maturity Level and Corresponding Narrative: ***Managed and Measurable (Level 4)*** - The organization measures the effectiveness of its awareness program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities?

Maturity Level and Corresponding Narrative: ***Defined (Level 2)*** – The organization has defined its security training policies, procedures, and related material based on FISMA requirements, its mission and risk environment, and the types of roles with significant security responsibilities. In addition, the organization has defined its processes for ensuring that personnel with assigned security roles and responsibilities are provided specialized security training [within organizationally defined time frames] and periodically thereafter.

Comments: The metric rating declined from *Managed and Measurable* to *Defined* due to a program level open weakness. The IRS has a program level weakness on not ensuring that training is required to be completed before system access and when there are significant changes to an information system environment or procedures. The IRS has requested policy changes, and if changed, will allow the IRS to close the program level weakness.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

Overall Security Training Maturity Level: ***Managed and Measurable (Level 4)*** – Based on the performance results for metrics 41 through 45, this function was evaluated at maturity level 4, *Managed and Measurable*.

Overall Security Training Maturity Comments: The IRS's security training program is effective because it meet the *Managed and Measurable* maturity level 4.

DETECT Function Area – 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 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 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 ISCM policies, procedures, and strategy.

Comments: Although the organization captures lessons learned to make improvements to ISCM policies and strategy, the IRS has not fully developed its audit logging. In addition, the IRS has not fully developed tools that support an accurate inventory. [REDACTED]


[REDACTED] The GAO reported that deficiencies continue to exist concerning inconsistent monitoring of systems and accounts, and out-of-date and unsupported hardware and software. In addition, the IRS has an open recommendation in a prior TIGTA report to ensure that the IRS completes the deployment of an automated asset discovery tool (or tools if needed) and builds an accurate and complete inventory of information technology assets (including hardware and software) that reside on the IRS network.

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

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

Comments: The IRS did not specifically address allocation of resources (people, processes, and technology) in a risk-based manner, and in addition, did not address accountability for carrying out roles and responsibilities effectively.

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?

Information Security Continuous Monitoring	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	0
Level 3: Consistently Implemented	1
Level 2: Defined	3 
Level 1: Ad Hoc	0

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: While the IRS has defined policies and procedures for security control assessments, we identified issues with the completeness and accuracy of the System Security Plans. For example, in the System Security Plan, controls did not have a status narrative, POA&M canceled in prior FISMA year was documented as open, and narrative identifying a weakness was documented as implemented in the control status. According to the IRS, it has and will continue to take steps to implement automation to improve security and provide a holistic view of risks identified during FISMA assessments.

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 expanded the scope of its dashboards and added new dashboards to allow for more data to be reported, information that feeds the dashboards is still not fully captured. [REDACTED]

Without capturing comprehensive data, the stakeholders cannot verify the data captured and validate the security posture across the organization.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

Overall ISCM Maturity Level: **Defined (Level 2)** – Based on the performance results for metrics 47 through 50, this function was evaluated at maturity level 2, *Defined*.

Overall ISCM Program Comments: The IRS's ISCM program is not effective because it did not meet the *Managed and Measurable* maturity level 4.



RESPOND Function Area – Incident Response

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

Maturity Level and Corresponding Narrative:

Consistently Implemented (Level 3) – The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary.

Comments: The IRS did not provide sufficient evidence supporting the *Managed and Measurable* maturity level 4 (ensuring that data supporting performance metrics are obtained accurately, consistently, and in a reproducible format).

 Incident Response	Count
Level 5: Optimized	1
Level 4: Managed and Measurable	3 
Level 3: Consistently Implemented	3
Level 2: Defined	0
Level 1: Ad Hoc	0

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: ***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 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,¹⁶ 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 IRS did not provide sufficient information to support that metrics are used to measure and manage the timely reporting of incident information. Although the IRS did supply specific information about reporting of individual incidents, including timeliness, it did not provide support that metrics derived from these incidents are summarized and used to measure and manage timely reporting (e.g., the number of incidents referred timely or the average time expended per referral for specific time periods).

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

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

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

- Web application protections, such as web application firewalls.
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools.
- Aggregation and analysis, such as security information and event management products.
- Malware detection, such as antivirus and antispam software technologies.
- Information management, such as data loss prevention.
- File integrity and endpoint and server security tools.

Maturity Level and Corresponding Narrative: ***Consistently Implemented (Level 3)*** – The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Comments: The metric rating declined from *Managed and Measurable* from Fiscal Year 2020 to *Consistently Implemented*, based on several factors. Although the IRS has implemented incident response technologies in the specified areas, there was insufficient information provided to support that they were interoperable to the extent practicable and

¹⁶ The United States Computer Emergency Response Team is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security.

that they cover all components of the organization's network. These items are required to meet the *Consistently Implemented* maturity level. In addition, TIGTA reported that the IRS's Endpoint Detection and Response solution was not at full operating capability on all eligible enterprise workstations, and initial deployment was limited to workstations and did not include servers. We took into consideration that this technology is currently being used in some capacity to support the incident response program; however, based on our audit results, it is not being utilized to the extent possible. Despite not fully meeting all requirements, we used our discretion to rate this metric as *Consistently Implemented*.

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. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?



Overall Incident Response Maturity Level: **Managed and Measurable (Level 4)** – Based on the performance results for metrics 52 through 58, this function was evaluated at maturity level 4, *Managed and Measurable*.

Overall Incident Response Program Comments: The IRS's incident response program is effective because it meet the *Managed and Measurable* maturity level 4.

RECOVERY Function Area – Contingency Planning

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

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

 Contingency Planning	Count
Level 5: Optimized	0
Level 4: Managed and Measurable	4 
Level 3: Consistently Implemented	1
Level 2: Defined	1
Level 1: Ad Hoc	0

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

Maturity Level and Corresponding Narrative: **Consistently Implemented (Level 3)** – The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission-essential functions/high-value assets.

Comments: In reference to metric 4, the IRS did not timely complete BIAs at the time of the information system contingency plan update.

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 is able to 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 System 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: **Defined (Level 2)** – The organization has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and Redundant Array of Independent Disks,¹⁷ as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment (e.g., cloud model deployed), maximum downtimes, recovery priorities, and integration with other contingency plans.

Comments: While IRS processes, strategies, and technologies for information system backup and storage (including use of alternate storage and processing sites) have been defined, it has not ensured that they are consistently implemented. [REDACTED]

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

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

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.

¹⁷ Redundant Array of Independent Disks are used to store the same data in different places on multiple hard disks to protect data in the case of a drive failure.

Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?

Overall Contingency Planning Maturity Level: ***Managed and Measurable (Level 4)*** – Based on the performance results for metrics 60 through 65, this function area was evaluated at a maturity level 4, *Managed and Measurable*.

Overall Contingency Planning Program Comments: The IRS's contingency planning program is effective because overall it met the *Managed and Measurable* maturity level 4.

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 2021 FISMA domain metrics. To accomplish our objective, we:

- Determined the maturity level for the metrics contained in the Fiscal Year 2021 Inspector General FISMA Reporting Metrics that pertain to nine security program components (*i.e.*, domains) and the associated number of metrics: Risk Management (10 metrics), SCRM (four metrics),¹ Configuration Management (eight metrics), Identity and Access Management (eight metrics), Data Protection and Privacy (five metrics), Security Training (five metrics), ISCM (four metrics), Incident Response (seven metrics), and Contingency Planning (six metrics). In addition to these metrics, each security program area had one final metric on the overall maturity level of the previous metrics within that area. This metric was used to cite additional information on the effectiveness (positive or negative) of the organization's program not included in the previous metrics.
- Determined the overall rating for each of the nine domains by a simple majority rule, whereby the most frequent maturity level across the metrics will serve as the domain rating. For example, if there are seven metrics in a domain, and the IRS receives *Defined* ratings for three of the metrics and *Managed and Measurable* ratings for four metrics, we would rate the domain rating as *Managed and Measurable*. The Fiscal Year 2021 Inspector General FISMA Reporting Metrics allowed for some discretion on maturity level ratings 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 Department of the Treasury as a whole. We used the information system inventory contained within the TFIMS 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 gets selected that was selected in the past three FISMA reviews, we reselected for that system.
- Considered the results of TIGTA audits whose results were applicable to the FISMA metrics that were performed, completed, or contained recommendations that were still open during the Fiscal Year 2021 FISMA evaluation period, as listed in Appendix II, as well as audit reports from the GAO that contained results applicable to the FISMA metrics.

¹ The SCRM area was a new domain in the Fiscal Year 2021 FISMA metric domains. To provide agencies with sufficient time to fully implement requirements and standards under this area, these new metrics were not considered in the maturity rating for the Identify function area.

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 May through September 2021. This report covers the Fiscal Year 2021 FISMA evaluation period of July 1, 2020, through June 30, 2021. We conducted this evaluation 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); Kent Sagara, Director; Joseph Cooney, Audit Manager; Midori Ohno, Lead Auditor; Charles Ekunwe, Senior Auditor; Cari Fogle, Senior Auditor, Cindy Harris, Senior Auditor; Steven Stephens, Senior Auditor; Ashley Weaver, Senior Auditor; Esther Wilson, Senior Auditor; and Linda Nethery, Senior Information Technology Specialist.

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: 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 executives, and comparing relevant data and evidence obtained to the Fiscal Year 2019 FISMA Evaluation Guide, version 2.0, developed by the Council of the Inspectors General on Integrity and Efficiency in collaboration with the OMB and the DHS.

Appendix II

Information Technology Security-Related Audits Considered During Our Fiscal Year 2021 Evaluation and the Metric(s) to Which They Apply

1. TIGTA, Report No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019) – Metric 3.
2. TIGTA, Report No. 2019-40-071, *Strengthened Validation Controls Are Needed to Protect Against Unauthorized Filing and Input of Fraudulent Information Returns* (Sept. 2019) – Metrics 30 and 31.
3. TIGTA, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020) – Metrics 30, 31, and 32.
4. TIGTA, Report No. 2020-20-012, *While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established* (Mar. 2020) – Metric 31.
5. TIGTA, Report No. 2020-20-033, *Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information* (July 2020) – Metrics 32 and 35.
6. TIGTA, Report No. 2020-20-036, *Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices* (Aug. 2020) – Metrics 30, 31, and 33.
7. TIGTA, Report No. 2020-20-044, *Legacy Systems Management Needs Improvement* (Aug. 2020) – Metric 1.
8. TIGTA, Report No. 2021-26-006, *Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated* (Dec. 2020) – Metrics 1 and 2.
9. TIGTA, Report No. 2021-20-003, *Security Controls Over Electronic Crimes Labs Need Improvement* (Dec. 2020) – Metrics 2, 3, 21, 32, 47, and 64.
10. TIGTA, Report No. 2021-25-025, *Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center* (May 2021) – Metrics 21 and 64.
11. TIGTA, Report No. 2021-20-024, *Improvements Are Needed to More [REDACTED] [REDACTED] the Virtual Host Infrastructure Platform* (June 2021) – Metrics 2 and 21.
12. TIGTA, Report No. 2021-20-056, *Laptop and Desktop Sanitization Practices Need Improvement* (Sept. 2021) – Metric 36.
13. TIGTA, Report No. 2021-20-063, *Enterprise Linux Platform Management Needs Improvement* (Sept. 2021) – Metrics 1, 2, and 21.

14. 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) – Metrics 3, 6, 32, and 58.
15. 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) – Metrics 6 and 36.
16. GAO, GAO-20-174, *Identity Theft: IRS Needs to Better Assess the Risks of Refund Fraud on Business-Related Returns* (Jan. 30, 2020) – Metric 5.
17. GAO, GAO-21-162, *Financial Audit: IRS's FY 2020 and FY 2019 Financial Statements* (Nov. 10, 2020) – Metrics 21, 33, and 47.
18. GAO, GAO-21-401R, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls* (May 4, 2021) – Metrics 5, 21, 30, 31, 32, and 33.

Appendix III

Abbreviations

BIA	Business Impact Analysis
CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
ICAM	Identity, Credential, and Access Management
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RBD	Risk-Based Decision
SCRM	Supply Chain Risk Management
TFIMS	Treasury FISMA Inventory Management System
TIC	Trusted Internet Connection
TIGTA	Treasury Inspector General for Tax Administration
VDP	Vulnerability Disclosure Policy



**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.