TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Fiscal Year 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act

September 25, 2020

Reference Number: 2020-20-073

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

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.

Redaction Legend:
2 = Law Enforcement Techniques/Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

To report fraud, waste, or abuse, please call us at 1-800-366-4484

HIGHLIGHTS: Fiscal Year 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act

Final Report issued on September 25, 2020
Reference Number 2020-20-073

Why TIGTA Did This Evaluation

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. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2020.

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 2019, the IRS received and processed more than 253 million Federal tax returns and supplemental documents, which includes 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 2020, the Inspector General FISMA metrics were 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 FISMA 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 3, *Consistently Implemented*.

As examples of specific metrics that were not considered effective, TIGTA found that the IRS could improve on tracking and reporting on up-to-date inventories over hardware and software assets, ensuring that 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 25, 2020

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 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act (Audit # 202020022)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2020. 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 2020 Annual Audit Plan and addresses the major management challenge of Security Over 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. We are also sending copies of this report to the IRS managers affected by the report.

If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. 113-283. This Act amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

Table of Contents

Appendices

Background

The Federal Information Security Modernization Act of 2014

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 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.

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. The DHS is responsible for the operational aspects of Federal cybersecurity, such as establishing Governmentwide incident response and operating the tool to collect FISMA metrics. 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. FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

FISMA oversight for the Department of the Treasury is performed by the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of Inspector General. TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while the Treasury Office of Inspector General is responsible for all other Treasury bureaus. The Treasury Office of Inspector General has overall responsibility to combine the results for all the Treasury bureaus into one report for the OMB.

IRS responsibilities

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 2019, the IRS received and processed more than 253 million Federal tax returns and supplemental documents, which includes a substantial amount of taxpayer personal and

[1] Pub. L. No. 113-283. This Act amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

financial information. As the 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 cyber threats by implementing security practices in planning, implementation, management, and operations. The Cybersecurity function is tasked with preserving the confidentiality, integrity, and availability of the IRS systems and its data.

Fiscal Year 2020 Inspector General FISMA Reporting Requirements

The Fiscal Year 2020 Inspector General FISMA Reporting Metrics were developed as a collaborative effort among the OMB, the DHS, and the Council of the Inspectors General on Integrity and Efficiency in consultation with the Federal Chief Information Officer Council. The Fiscal Year 2020 metrics represent a continuation of work that began in Fiscal Year 2016 to align the Inspector General metrics with the five Cybersecurity Framework 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 components (or metric domains).

Figure 1: Alignment of the NIST Cybersecurity Framework's Function Areas to the Fiscal Year 2020 Inspector General FISMA Metric Domains

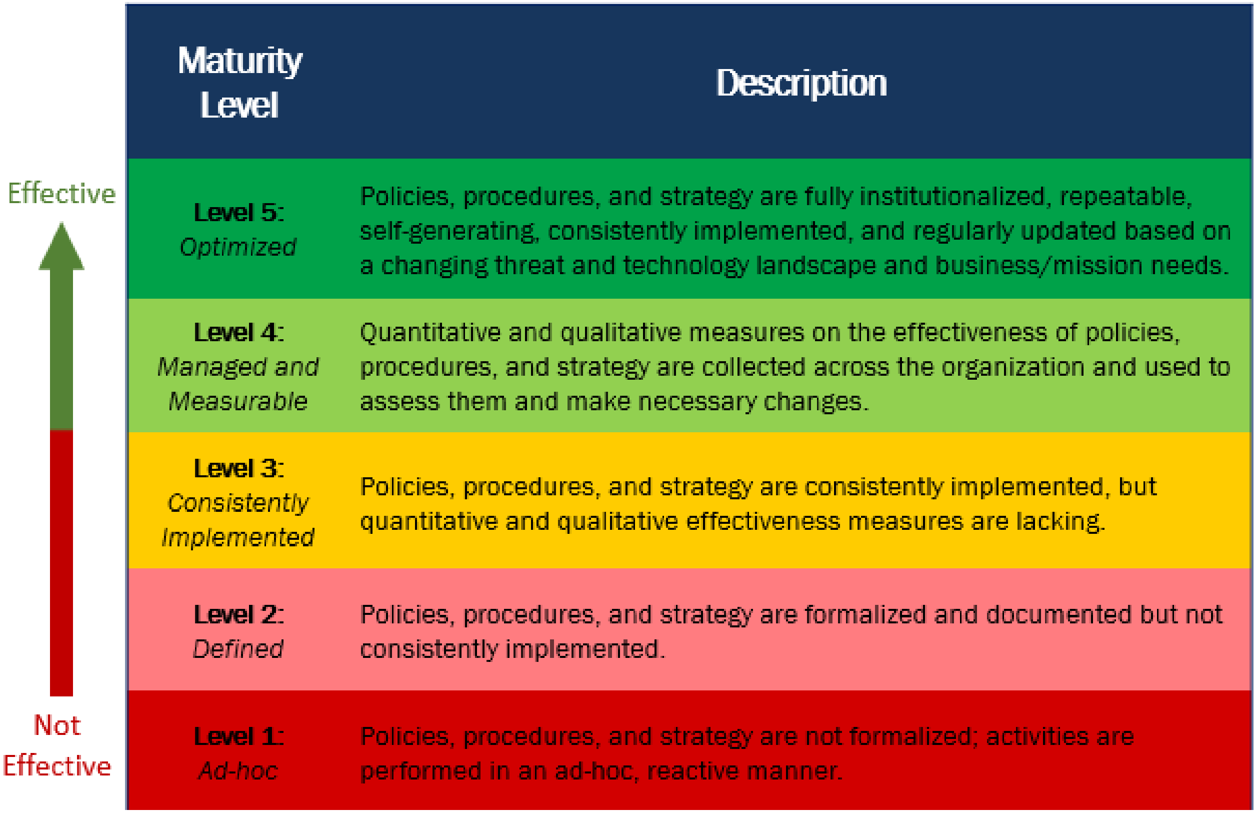
Function Areas	Cybersecurity Function Objective	Fiscal Year 2020 Inspector General FISMA Metric Domains
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Risk Management
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring (ISCM)
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Incident Response
RECOVER	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.	Contingency Planning

Source: Fiscal Year 2020 Inspector General FISMA Reporting Metrics and NIST Framework for Improving Critical Infrastructure Cybersecurity.

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

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.

Figure 2: Inspector General's Assessment Maturity Levels


Effective
Not Effective

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

Source: Fiscal Year 2020 Inspector General FISMA Reporting Metrics.

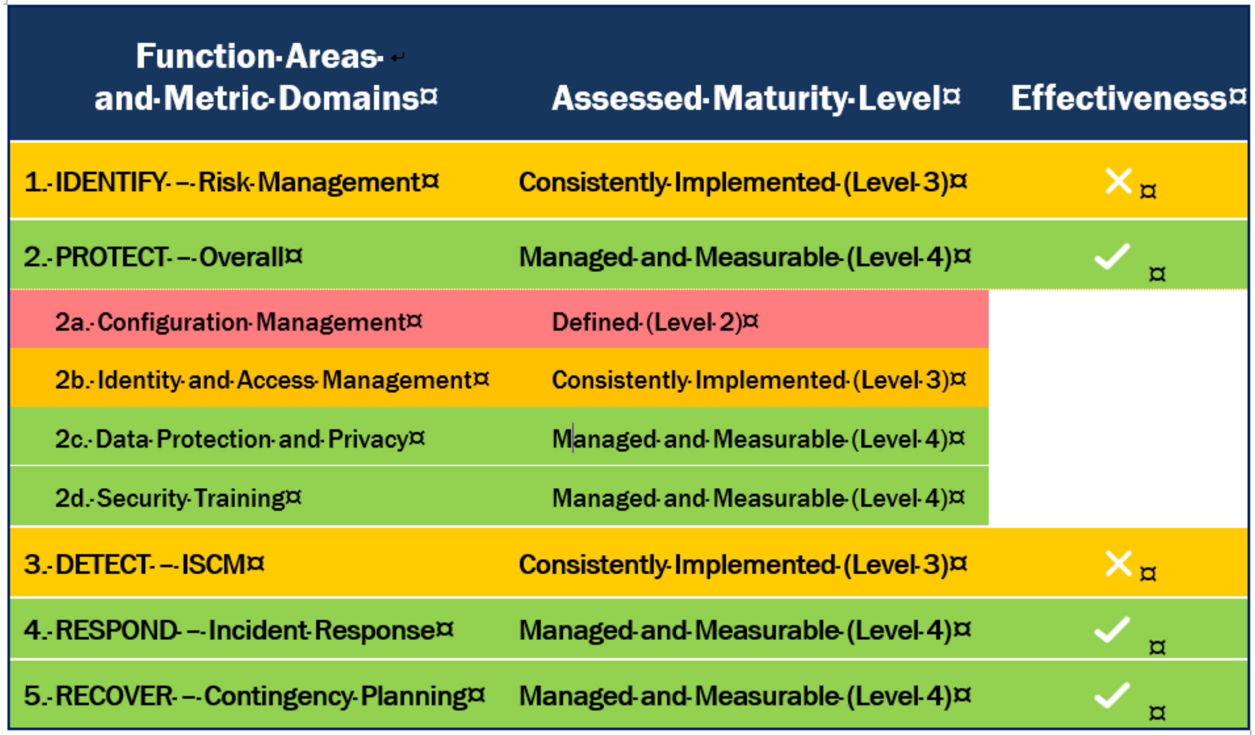
Results of Review

The Cybersecurity Program Was Not Fully Effective in Two 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 in the *Fiscal Year 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 4.0* (April 17, 2020). Along with our review of pertinent documents and discussions with IRS subject matter experts, we based our evaluation on a representative subset of seven information systems and the implementation status of key security controls as well as considered the results of TIGTA and Government Accountability Office (GAO) audits. These audits, whose results were applicable to the FISMA metrics, were performed, completed, or contained recommendations that were still open during the FISMA evaluation period (July 1, 2019, to June 30, 2020). See Appendix II for a list of these audits with notations on the metric(s) to which each report 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



Function Areas and Metric Domains	Assessed Maturity Level	Effectiveness
1. IDENTIFY – Risk Management	Consistently Implemented (Level 3)	✗
2. PROTECT – Overall	Managed and Measurable (Level 4)	✓
2a. Configuration Management	Defined (Level 2)	
2b. Identity and Access Management	Consistently Implemented (Level 3)	
2c. Data Protection and Privacy	Managed and Measurable (Level 4)	
2d. Security Training	Managed and Measurable (Level 4)	
3. DETECT – ISCM	Consistently Implemented (Level 3)	✗
4. RESPOND – Incident Response	Managed and Measurable (Level 4)	✓
5. RECOVER – Contingency Planning	Managed and Measurable (Level 4)	✓

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 2020 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 2020 Inspector General FISMA Reporting Metrics. Details of the results of our evaluation of these maturity levels are presented on pages 23 and 25.

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 2020 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 a result, 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 and is considered "effective" in accordance with the Fiscal Year 2020 Inspector General FISMA Reporting Metrics. Details of the results of our evaluation of these maturity levels are presented on pages 11, 14, 17, and 19.

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 17 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 19 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 *Consistently Implemented* maturity level

Based on the Fiscal Year 2020 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 *Consistently Implemented* maturity level 3, which we considered "not effective" in accordance with the Fiscal Year 2020 Inspector General FISMA Reporting Metrics. Details of our evaluation are presented on pages 6 and 21. The following examples are metrics that did not meet the *Managed and Measurable* maturity level 4.

- Metrics 2 and 3 pertain to tracking and reporting on an up-to-date inventory of hardware and software assets, respectively. To address deficiencies on accurately accounting for its hardware inventory, the IRS deployed an information technology asset management platform that enables a reconciliation of asset inventory and significantly improves data accuracy. However, the IRS will not fully implement this platform until Fiscal Year 2021. This platform will also play a key role in maintaining information on software assets. In addition, we found that the IRS has a Plan of Action and Milestones (POA&M) which documents open hardware and software inventory weaknesses.
- Metric 46 pertains to the ISCM strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM. The IRS has developed the ISCM strategy, but the strategy did not include vulnerability

scanning *********************************2***
***************************2************************.

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.

TIGTA's responses to the Fiscal Year 2020 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the Fiscal Year 2020 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[3] 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 2020 Inspector General FISMA Reporting Metrics.

Function Area 1 – IDENTIFY (Risk Management)

Risk Management	Count
Level 5: Optimized	0
Level 4: Managed & Measurable	3
Level 3: Consistently Implemented	6 ⊗
Level 2: Defined	4
Level 1: Ad-hoc	0

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: ***Defined*** **(Level 2)** – The organization has defined a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.

   Comments: The IRS uses multiple systems to track system inventory. However, we have limited assurance that the IRS maintains a comprehensive and accurate inventory of its information systems. For example, the confusion and uncertainty caused by the IRS on providing information for this metric gave us limited assurance as to the reliability and accuracy of the end result of public-facing websites. In addition, another TIGTA audit team experienced many challenges in trying to determine the number of IRS applications that store and process taxpayer data and Personally Identifiable Information. Lastly, TIGTA reported that the IRS does not have a complete and accurate inventory of legacy systems.

2. To what extent does the organization use standard data elements/taxonomy[4] to develop and maintain an up-to-date inventory of hardware assets (including Government-Furnished Equipment and Bring Your Own Device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

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

[4] Taxonomy is a scheme of classifications.

Maturity Level: ***Defined*** **(Level 2)** – The organization has defined a process 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: TIGTA found that the IRS has a POA&M that documents an open hardware inventory weakness as the IRS has not identified all of its current system hardware components. TIGTA also reported that mainframe hardware asset and wireless access point inventories were inaccurate and incomplete. Further, the GAO reported that the IRS did not correct deficiencies on out-of-date and unsupported hardware. In March 2020, the IRS deployed an information technology asset management use case tool that enabled a scalable platform hosting data populated with asset data from four sources to reconcile asset inventory and significantly improved data accuracy. The IRS anticipates fully deploying this platform during Fiscal Year 2021.

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: ***Defined*** **(Level 2)** – The organization has defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.

   Comments: The IRS has an open POA&M that documents a weakness whereby the IRS is not able to detect unauthorized software. The information technology asset management platform mentioned in metric 2 will also play a key role in developing and maintaining an up-to-date inventory of software assets.

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: ***Managed and Measurable*** **(Level 4)** – The organization ensures the risk-based allocation of resources for the protection of high-value assets through collaboration and data-driven prioritization.

5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management? This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk.

   Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination of the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program. In accordance with the SECURE Technology Act,[5] the organization is taking measurable steps to implement its action plan for supply chain risk management.

Comments: For Fiscal Year 2020, the IRS provided an enterprise-wide response; however, the metric rating declined from Managed and Measurable to Consistently Implemented due to the requirement addressing the SECURE Technology Act of 2018 provisions for supply chain risk management. The Act established the Federal Acquisition Security Council, which later issued a Strategic Plan in June 2020 for executive agencies to use as a framework for their supply chain risk management strategy. As a result, the IRS could not take measurable steps addressing the Act during the Fiscal Year 2020 FISMA evaluation year. The IRS did provide a timeline to show that it is actively participating in the Treasury Strategic Supply Chain Management and Oversight process since July 2020. According to the IRS, going forward, the Department of the Treasury will provide bureaus with implementable policies and procedures to deploy supply chain risk management best practices and methodology.

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

   Comments: While the IRS has implemented the information security architecture, the IRS did not always integrate the Enterprise Life Cycle process into its system and program. TIGTA reported that the IRS did not establish an effective governance structure nor a suitable development methodology for automation projects. In another instance, TIGTA reported that IRS did not complete the Enterprise Life Cycle methodology artifacts.

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

   Maturity Level: ***Managed and Measurable*** **(Level 4)** – Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement risk management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. In addition, the organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.

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

   Maturity Level: ***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.

[5] Pub. L. No. 115-390, 132 Stat 5173.

Comments: To be at the *Consistently Implemented* maturity level 3, the IRS should consistently use POA&Ms to effectively mitigate security weaknesses. We reviewed 55 POA&Ms that were closed in Fiscal Year 2020 related to the seven systems. Of those POA&Ms, we found 10 POA&Ms that were closed without sufficient support showing that the weaknesses were corrected, even though the IRS had validated the closures through its closure verification process. The IRS provided additional evidence to support four POA&M closures and reopened one POA&M after we brought it to the IRS's attention. ******2******
2*
without corresponding POA&Ms on two of the seven information systems we reviewed. *2*
2*
2****************************. The IRS has not yet initiated its review of the canceled POA&M as of this review. Without POA&Ms, there is no mechanism to ensure that these vulnerabilities are remediated. In addition, TIGTA reported that the IRS did not always track audit trail deficiencies in a POA&M and did not timely resolve security weaknesses related to its wireless network.

9. To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system-level risk assessments, including for identifying and prioritizing: (i) internal and external threats, including through use of the common vulnerability scoring system or other equivalent framework; (ii) internal and external asset vulnerabilities, including through vulnerability scanning; (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities; and (iv) security controls to mitigate system-level risks?

Maturity Level: ***Consistently Implemented*** **(Level 3)** – System risk assessments are performed and appropriate security controls are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities.

Comments: Vulnerability scan reports provided for the seven information systems we reviewed contained information on the severity of the vulnerabilities. System risk assessments were performed on the seven systems; however, we noticed issues with the completeness and adequacy of the security documents. For example, the failed controls were not properly included or updated in the System Security Plan or the Security Assessment Report. Further, TIGTA reported that the Unified Access Project team had not completed the required Enterprise Life Cycle methodology, specifically the System Security Plan and Information Systems Contingency Plan, and the Identity Service Engine software was not included in the authorization boundary of a general support system. In reference to the above TIGTA report, the IRS stated that it had resolved and closed the issue on August 20, 2020, which was outside of the FISMA cycle.

10. To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders?

Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization ensures that information about risks is communicated in a timely and consistent manner to all 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: According to the IRS, the Continuous Diagnostics and Mitigation Phase 1 was declared complete as of May 1, 2020. However, the information that feeds the Continuous Diagnostics and Mitigation dashboards are still not perfected. Without a complete and accurate collection of data, the IRS does not have a portfolio view of interrelated risks across the enterprise. For example, the IRS has not completed implementing database scans. **2** ***2**

Further, TIGTA rated the inventory metrics above (metrics 1, 2, and 3) at a *Defined* maturity level 2, which means the IRS has not effectively identified and maintained these inventory areas, thus making it difficult to determine the specific risks of any unknown inventory items.

11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation[6] clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements[7] are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services?

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization uses qualitative and quantitative performance metrics (*e.g.*, those defined within Service Level Agreements) to measure, report on, and monitor information security performance of contractor-operated systems and services.

12. To what extent does the organization utilize technology (such as a governance, risk management, and a compliance tool) to provide a centralized, enterprise-wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

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

    Comments: While the IRS consistently implemented a solution that provides a centralized enterprise-wide view of risks, the information provided did not support cyber threat modeling. Specifically, the documents provided by the IRS did not substantiate that it utilizes cyber threat modeling as a component of cyber risk framing, analysis and assessment, and evaluation of alternative responses (individually or in the context of cybersecurity portfolio management).

13. 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: ***Consistently Implemented*** **(Level 3)** – Based on the performance results for metrics 1 through 12, this function area was evaluated at maturity level 3, *Consistently Implemented*.

[6] The Federal Acquisition Regulation is the primary regulation for use by all Federal executive agencies in their acquisition of supplies and services with appropriated funds.

[7] A Service Level Agreement is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider will meet.

Overall Risk Management Program Comments: The IRS risk management program is not effective because it did not meet the *Managed and Measurable* maturity level 4.

Function Area 2a – PROTECT (Configuration Management)

Configuration Management	Count
Level 5: Optimized	0
Level 4: Managed & Measurable	1
Level 3: Consistently Implemented	2
Level 2: Defined	5 ⊗
Level 1: Ad-hoc	0

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

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

    Comment: 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. The IRS self-reported as this maturity level, and we agreed with the IRS's self-assessment.

15. 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;[8] configuration monitoring; and applying configuration management requirements to contractor-operated systems?

    Maturity Level: *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.

16. To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: The maturity level should take into consideration the maturity of questions 17, 18, 19, and 21.)

    Maturity Level: *Defined* **(Level 2)** – The organization has developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements.

    Comments: While the IRS has defined policies and procedures for managing the configurations of its information systems, it has not consistently implemented its policies and procedures, based on the maturity levels of metrics 17, 18, 19, and 21.

[8] 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.

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

    Comments: 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. The IRS's annual security testing of systems reported that two of the seven information systems we reviewed did not maintain configuration baselines. In addition, three information systems did not maintain and keep up-to-date information system component inventories. Further, the IRS has not implemented the tools necessary to perform checks for unauthorized components/devices and to notify appropriate organizational officials. In addition, TIGTA reported many instances of baseline configurations not being consistently implemented or inaccurate system component inventories.

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

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

    Comments: While the IRS has defined common secure configurations, it has not ensured that its information systems consistently maintain secure configuration settings in compliance with IRS policy. The IRS's annual security testing of systems reported that four information systems we reviewed did not maintain secure configuration settings in accordance with IRS policy. Also, least functionality controls were not fully in place for three information systems. In addition, vulnerability scanning and flaw remediation controls were not fully in place for three information systems. Furthermore, the IRS is awaiting the selection, implementation, and configuration of a software tool by the DHS that will prevent program execution. In addition, TIGTA and the GAO reported control deficiencies in either secure configuration settings, least functionality, vulnerability scanning, or flaw remediation.

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

    Maturity Level: ***Defined*** **(Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws; testing software and firmware updates prior to implementation; installing security-relevant updates and patches within organizationally defined time frames; 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. The IRS's annual security testing of systems reported that configuration change control was not fully in place for four information systems we review. In addition, vulnerability scanning and flaw remediation controls were not fully in place for three information systems, and malicious code protection controls were not fully in place for two information systems. In addition, both TIGTA and the GAO reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner.

20. To what extent has the organization adopted the Trusted Internet Connection program to assist in protecting its network?

    Maturity Level: *Consistently Implemented* **(Level 3)** – The organization has consistently implemented its Trusted Internet Connection–approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined Trusted Internet Connection security controls, as appropriate, and implemented actions to ensure 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, the IRS's DHS-approved Trusted Internet Connection up to version 2.0. However, the IRS has not defined its plans for meeting the goals of the Trusted Internet Connection 3.0 initiative. The IRS stated that it is aware and monitoring the Cybersecurity and Infrastructure Security Agency's status for future Trusted Internet Connection 3.0 use cases.

21. 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,[9] as appropriate?

    Maturity Level: *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 policy and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that two information systems we reviewed did not maintain configuration baselines, and configuration change control was not fully in place for four information systems. Also, security impact analysis control is not fully in place for two information systems. In addition, TIGTA and the GAO reported that the IRS did not follow its change management policy and procedures.

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

[9] 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 life cycle of an information system.

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 14 through 21, this function area was evaluated at a maturity level 2, *Defined*.

Overall Configuration Management Program Comments: The IRS configuration management program is not effective because it did not meet the *Managed and Measurable* maturity level 4. The IRS stated that its Configuration Management Dashboard was implemented on April 20, 2020, using data from the BigFix tool, the Knowledge, Incident/Problem Service Asset Management system, and the Hewlett-Packard Universal Configuration Management database. The Defense Information System Agency's Security Technical Implementation Guides, in conjunction with the IRS's Internal Revenue Manuals, are used as the standard baselines. The dashboard is available for use at an enterprise level to help drive risk remediation for assets. A feature of the dashboard to help assess maturity is the trending views presented at the operating system and device levels, which give the IRS a better picture of the changing environment and the impact of remediation efforts in place.

Function Area 2b – PROTECT (Identity and Access Management)

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

23. To what degree have the roles and responsibilities of identity, credential, and access management stakeholders been defined, communicated across the agency, and appropriately resourced?

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

24. To what degree does the organization utilize an identity, credential, and access management strategy to guide its identity, credential, and access management processes and activities?

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization is consistently implementing its Identity, Credential, and Access Management strategy and is on track to meet milestones. The strategy encompasses the entire organization; aligns with the Federal Identity, Credential, and Access Management and Continuous Diagnostic and Mitigation requirements; and incorporates applicable Federal policies, standards, playbooks, and guidelines.

    Comments: The Treasury Enterprise Identity, Credential, and Access Management office is preparing to roll out Phase 2 of the DHS's Continuous Diagnostics and Mitigation program. The IRS is following the Treasury Enterprise Identity, Credential, and Access Management roadmap and business case to guide its efforts and show progress in meeting milestones. The IRS self-reported as this maturity level, and we agreed with the IRS's self-assessment.

25. To what degree have identity, credential, and access management policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31.)

Maturity Level: *Consistently Implemented* **(Level 3)** – The organization consistently implements its policies and procedures for Identity, Credential, and Access Management, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its Identity, Credential, and Access Management policies, procedures, and processes to update the program. The organization ensures that there is consistent coordination amongst organization leaders and mission owners to implement, manage, and maintain the organization's Identity, Credential, and Access Management policies, processes, and technologies.

Comments: While the IRS has developed, documented, and disseminated its policies and procedures for Identity, Credential, and Access Management, based on the maturity levels of metrics 26 through 31, the IRS has not collectively met the *Managed and Measurable* maturity level 4 for this metric.

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

27. 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: *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.

28. 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 non-privileged users to access the organization's facilities, networks, and systems, including for remote access?

    Maturity Level: *Defined* **(Level 2)** – The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's facilities, systems, and networks, including the completion of e-authentication risk assessments.

    Comments: The IRS's annual security testing of systems reported that the authenticator management control is not fully in place for three information systems we reviewed. In addition, the identification and authentication (organizational users) control is not fully in place for four information systems. Further, both TIGTA and the GAO reported authentication weaknesses. Finally, while the IRS reported that 92 percent of its non-privileged users are required to use Personal Identity Verification cards to access the network, it also reported that only 79 (59 percent) of 134 internal systems are configured to require Personal Identity Verification cards.

29. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access?

    Maturity Level: ***Defined* (Level 2)** – The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's facilities, systems, and networks, including the completion of electronic authentication risk assessments.

    Comments: While the IRS reported that 100 percent of its privileged users are required to use Personal Identity Verification cards to access the network, it reported that only 79 (59 percent) of 134 internal systems are configured to require Personal Identity Verification cards. In addition, TIGTA and the GAO reported authentication weaknesses, as presented in metric 28.

30. 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: ***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. Both TIGTA and the GAO reported control deficiencies that included unnecessary access rights granted to accounts, lack of segregation of duties, and inconsistent monitoring of systems and accounts. In addition, the IRS annual security testing of systems reported that account management control is not fully in place for five information systems we reviewed; separation of duties control is not fully in place for two information systems; least privilege control is not fully in place for three information systems; audit review, analysis, and reporting control is not fully in place for five information systems; and identifier management control is not fully in place for three information systems. Also, the Organizational Common Controls Security Plan shows that audit review, analysis, and reporting control is not fully in place.

31. 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: ***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 140-2[10] on all of its remote access

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

connections. In addition, the IRS's annual security testing of systems reported that cryptographic module authentication control is not fully in place for two information systems we reviewed; network disconnect control is not fully in place for two information systems; and cryptographic protection control is not fully in place for five information systems. Further, both TIGTA and the GAO reported inadequate use of encryption to protect systems and data.

32. 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 23 through 31, this function area was evaluated at a maturity level 2, *Defined*. However, the Fiscal Year 2020 Inspector General FISMA Reporting Metrics allows 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 Identity and Access Management Program is not effective because several significant deficiencies related to computer security have been identified for the IRS in this area and indicate pervasive, organization-wide deficiencies that may impact all of the IRS systems. As such, the IRS did not meet the *Managed and Measurable* maturity level 4.

Function Area 2c – PROTECT (Data Protection and Privacy)

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

33. 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: ***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, 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. While it maintains a system to track this information, there is limited assurance that the information maintained in that system is complete. Specifically, TIGTA reported that the IRS has no complete inventory of systems that maintain PII. In addition, TIGTA reported the IRS could not provide an accurate inventory for all applications that store or process taxpayer data and PII.

34. 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: ***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: The IRS has not yet deployed the Data at Rest component of the Data Loss Prevention solution, which is meant to identify PII and other sensitive information for encryption. In addition, the IRS did not provide sufficient evidence to support that media containing PII or sensitive data are destroyed as required. Lastly, the security control for System and Communications Protection–8 (transmission confidentiality and integrity) was not fully in place for two information systems we reviewed.

35. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?

    Maturity Level: ***Consistently Implemented* (Level 3)** – The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing and malware and blocks against known malicious sites. In addition, 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, audits its Domain Name System[11] records, 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, or that it conducts exfiltration exercises for, its enhanced network defenses. It also did not provide sufficient evidence that its Domain Name System infrastructure is being monitored for potential tampering in accordance with its ISCM strategy.

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

    Maturity Level: ***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.

37. To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974[12] and E-Government Act of 2002,[13] consequences for failing to carry out responsibilities,

[11] A device to access Internet resources by user-friendly domain names rather than Internet Protocol addresses; users need a system that translates these domain names to Internet Protocol addresses and back.

[12] 5 U.S.C. § 552a (2013).

[13] Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2899.

identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections, and use requirements.)

Maturity Level: ***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. In addition, the organization updates its program based on statutory, regulatory, mission, program, business process, and information system requirements and results from monitoring and auditing.

38. 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?

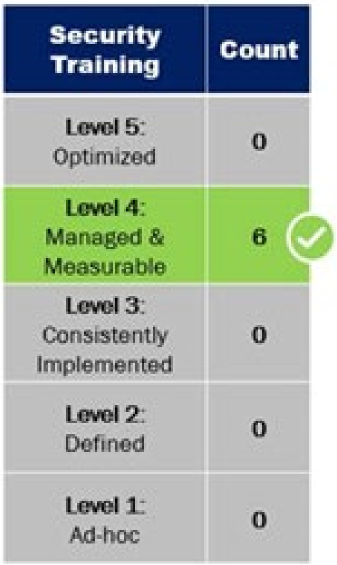
Overall Data Protection and Privacy Maturity Level: ***Managed and Measurable*** **(Level 4)** – Based on the performance results for metrics 33 through 37, this function area was evaluated at a maturity level 4, *Managed and Measurable*.

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

Function Area 2d – PROTECT (Security Training)

39. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated 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: ***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. This is the highest maturity level for this metric.



Security Training	Count
Level 5: Optimized	0
Level 4: Managed & Measurable	6 ✓
Level 3: Consistently Implemented	0
Level 2: Defined	0
Level 1: Ad-hoc	0

40. 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: ***Managed and Measurable*** **(Level 4)** – The organization has addressed its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors.

41. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: The strategy/plan should include the following components: the structure of the awareness and

training program, priorities, funding, 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, and phishing simulation tools), frequency of training, and deployment methods.)

Maturity Level: ***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.

42. To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: The maturity level should take into consideration the maturity of questions 43 and 44 below.)

Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

43. To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting.)

Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness, training, or disciplinary action, as appropriate.

44. To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures)?

Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness, training, or disciplinary action, as appropriate.

45. 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 39 through 44, this function area was evaluated at a maturity level 4, *Managed and Measurable*.

Overall Security Training Program Area Program Comments: The IRS security training program is effective because overall it met the *Managed and Measurable* maturity level 4.

Function Area 3 – DETECT (ISCM)

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

46. To what extent does the organization utilize an ISCM strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM?

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization's ISCM strategy is consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.

    Comments: The IRS has developed the ISCM strategy, ****2****
**********************************2********************************
**********************************2********************************
************2************.

47. To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security-related information required for metrics, assessments, and reporting; and analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy.

    Maturity Level: ***Defined*** **(Level 2)** – The organization's ISCM 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 requirements.

    Comments: Databases are not fully scanned throughout the IRS. In addition, three TIGTA reports identified a weakness in the identification and assessment of assets. Further, a GAO report identified new and continuing deficiencies in information system security controls that includes configuration management, information security management program, and audit and monitoring issues as well as a finding related to boundary protection. Finally, the IRS is not effectively monitoring key networks and systems to identify unauthorized activities and inappropriate system configurations.

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

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

    Comments: The IRS has improved its dashboards in this area; however, it is an ongoing process. The IRS improved by hiring 78 more employees to fill role-based positions; however, the employees were not proficient in five needed skills.

49. How mature are the organization's processes for performing ongoing assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls?

Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture as well as each system's contribution to said security posture. All security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status is updated regularly (as defined in the agency's information security policy) in security plans.

Comments: The IRS is consistently conducting security control assessments; however, the continuous monitoring controls are not always in place.

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

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

    Comments: Although the dashboards for this area have improved, the Continuous Diagnostic and Mitigation solution and the new Cyber Security Assessment and Monitoring tool are still being developed. Information that feeds the dashboards is still not perfected. The hardware and software inventories are still not consistently reported, and vulnerability scanning, audit trails, and patching are deficient. The IRS has an ISCM program plan in place to implement more tools and increase the metrics that are fed to the dashboards to achieve data collection, storage, analysis, retrieval, and reporting.

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: ***Consistently Implemented*** **(Level 3)** – Based on the performance results for metrics 46 through 50, this function area was evaluated at a maturity level 3, *Consistently Implemented*.

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

Function Area 4 – RESPOND (Incident Response)

Incident Response	Count
Level 5: Optimized	1
Level 4: Managed & Measurable	4 ✓
Level 3: Consistently Implemented	2
Level 2: Defined	0
Level 1: Ad-hoc	0

52. To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events? (Note: The overall maturity level should take into consideration the maturity of questions 53 through 58).

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy, and processes to update the program.

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

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

    Maturity Level: ***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. This is the highest maturity level for this metric.

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

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – 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. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems. This is the highest maturity level for this metric.

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

    Maturity Level: ***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: ***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 Response Team,[14]

[14] 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.

law enforcement, the Office of Inspector General, and Congress (for major incidents) in a timely manner.

Comments: The IRS did not provide sufficient evidence to support the *Managed and Measurable* maturity level 4; for example, to support the verification or validation of data used for performance measure metrics related to security incident containment and eradication activities.

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: ***Managed and Measurable* (Level 4)** – The organization utilizes Einstein 3 Accelerated to detect and proactively block cyberattacks or prevent potential compromises. This is the highest maturity level for this metric.

58. To what degree 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: ***Managed and Measurable* (Level 4)** – The organization uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.

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 area was evaluated at a maturity level 4, *Managed and Measurable*.

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

Function Area 5 – RECOVER (Contingency Planning)

Contingency Planning	Count
Level 5: Optimized	0
Level 4: Managed & Measurable	5 ✓
Level 3: Consistently Implemented	1
Level 2: Defined	1
Level 1: Ad-hoc	0

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

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

61. To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62 through 66.)

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization understands and manages its information and communications technology supply chain risks related to contingency planning activities. As appropriate, the organization integrates information and communication technology supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its information and communication technology supply chain infrastructure, applies appropriate information and communication technology supply chain controls to alternate storage and processing sites, and considers alternate telecommunication service providers for its information and communication technology supply chain infrastructure and to support critical information systems.

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

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization consistently incorporates the results of organizational and system-level business impact analyses into strategy and plan development consistently. System-level business impact analyses are integrated with the organizational-level business impact analyses 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 business impact analyses are consistently used to determine contingency planning requirements and priorities, including mission-essential functions and high-value assets. This is the highest maturity level for this metric.

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

    Maturity Level: ***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.

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

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

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

    Maturity Level: ***Defined*** **(Level 2)** – Processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and Redundant Array of Independent Disks,[15] as appropriate, have been defined. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, maximum downtimes, recovery priorities, and integration with other contingency plans.

    Comments: While the IRS has robust processes for contingency planning, it did not consistently implement these processes. During Fiscal Year 2020, the IRS incorporated semiannual testing of backup information for systems with a moderate security classification and quarterly testing for systems with a high-security classification, which resulted in a 76 percent completion rate. The IRS's goal is to be in full compliance in Fiscal Year 2021. In addition, the IRS's annual security testing of information systems we reviewed had a weakness with one or more controls pertaining to the alternate storage site, alternate processing site, telecommunications services, and information system backups for four information systems.

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

    Maturity Level: ***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 are obtained accurately, consistently, and in a reproducible format. This is the highest possible rating for this metric.

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

    Overall Contingency Planning Maturity Level: ***Managed and Measurable*** **(Level 4)** – Based on the performance results for metrics 60 through 66, this function area was evaluated at a maturity level 4, *Managed and Measurable*.

[15] A Redundant Array of Independent Disks is used to store the same data in different places on multiple hard disks to protect data in the case of a drive failure.

Overall Contingency Planning Program Comments: The IRS 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. To accomplish our objective, we:

- Determined the maturity level for the metrics contained in the Fiscal Year 2020 Inspector General FISMA Reporting Metrics that pertain to eight security program components and the associated number of metrics: Risk Management (12 metrics), Configuration Management (8 metrics), Identity and Access Management (9 metrics), Data Protection and Privacy (5 metrics), Security Training (6 metrics), ISCM (5 metrics), Incident Response (7 metrics), and Contingency Planning (7 metrics). In addition to the above metrics, each security program area has one final metric on the overall maturity level of the previous metrics within that area. This may also include additional information on the effectiveness (positive or negative) of the organization's program not included in the above metrics.
- Determined the overall rating for each of the eight 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*.
- Based our evaluation work, in part, on a representative subset of seven IRS information systems. To select the representative subset of the information 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 Treasury FISMA Inventory Management System of general support systems, major applications, and minor applications with a security classification of moderate or high as the population for this subset. We used a random number table to select information systems within this population. Generally, if an information system 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 2020 FISMA evaluation period, as listed in Appendix II, as well as audit reports from the GAO that contained results applicable to the FISMA metrics.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity function in the New Carrollton Federal Building in Lanham, Maryland, during the period May through September 2020. This report covers the Fiscal Year 2020 FISMA evaluation period of July 1, 2019, through June 30, 2020.

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; Steven Stephens, 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 objective: NIST Special Publication 800-53 and Internal Revenue Manual policies related to information technology security controls. We evaluated these controls by reviewing documentation provided by the IRS 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 2020 Evaluation and the Metric(s) to Which They Apply

1. TIGTA, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies* (Sept. 2011) – Metrics 18 and 19.
2. TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012) – Metrics 18 and 19.
3. TIGTA, Ref. No. 2012-20-112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012) – Metric 17.
4. TIGTA, Ref. No. 2012-20-122, *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements* (Sept. 2012) – Metrics 18 and 19.
5. TIGTA, Ref. No. 2014-23-072, *Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project* (Sept. 2014) – Metrics 18 and 19.
6. TIGTA, Ref. No. 2016-20-050, *Significant Improvements Are Needed to the Mainframe Computing Environment Security* (July 2016) – Metrics 18, 19, 27, and 30.
7. TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018) – Metric 17.
8. TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019) – Metric 17.
9. TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019) – Metric 17.
10. TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019) – Metrics 17, 21, and 30.
11. TIGTA, Ref. No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019) – Metric 33.
12. TIGTA, Ref. No. 2019-40-071, *Strengthened Validation Controls Are Needed to Protect Against Unauthorized Filing and Input of Fraudulent Information Returns* (Sept. 2019) – Metrics 28 and 29.
13. TIGTA, Ref. No. 2020-40-004, *Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites* (Nov. 2019) – Metric 31.
14. TIGTA, Ref. No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020) – Metrics 18, 19, 28, 29, and 30.

15. TIGTA, Ref. 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) – Metrics 28 and 29.
16. TIGTA, Ref. No. 2020-20-013, *The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data* (Mar. 2020) – Metric 10, 17, 18, and 47.
17. TIGTA, Ref. 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 1, 8, 17, 30, and 47.
18. TIGTA, Ref. 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 6, 9, and 30.
19. TIGTA, Ref. No. 2020-20-043, *Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed* (Aug. 2020) – Metric 47.
20. TIGTA, Ref. No. 2020-20-044, *Legacy Systems Management Needs Improvement* (Aug. 2020) – Metrics 1 and 17.
21. TIGTA, Ref. No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020) – Metrics 2, 17, 18, 19, and 31.
22. TIGTA, Ref. No. 2020-20-060, *Process Automation Benefits Are Not Being Maximized, and Development Processes Need Improvement* (Sept. 2020) – Metric 6.
23. TIGTA, Ref. No. 2020-20-063, *Improvements Are Needed to Ensure Wireless That Networks Are Secure* (Sept. 2020) – Metrics 2, 8, 17, 19, and 30.
24. GAO, GAO-20-159, *Financial Audit: IRS's Fiscal Year 2019 and Fiscal Year 2018 Financial Statements* (Nov. 2019) – Metrics 2, 18, 19, 21, 28, 29, 30, 31, and 47.
25. GAO, GAO-20-411R (and GAO-20-410RSU), *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (May 2020) – Metrics 18, 19, 21, 28, 29, 30, 31, and 47.

Appendix III

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration