TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Fiscal Year 2019 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act

September 24, 2019

Reference Number: 2019-20-082

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.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

FISCAL YEAR 2019 EVALUATION OF THE INTERNAL REVENUE SERVICE'S CYBERSECURITY PROGRAM AGAINST THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Highlights

Final Report issued on September 24, 2019

Highlights of Reference Number: 2019-20-082 to the Department of the Treasury, Office of Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Federal Information Security Modernization Act of 2014 (FISMA) focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. 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.

WHY TIGTA DID THE AUDIT

As part of the 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. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2019.

WHAT TIGTA FOUND

For Fiscal Year 2019, the Inspector General FISMA reporting was aligned with the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and measured the maturity levels for five function areas: IDENTIFY (organizational understanding to manage cybersecurity risk to assets and capabilities), PROTECT (appropriate safeguards to ensure delivery of critical services), DETECT (appropriate activities to identify the occurrence of a cybersecurity event), RESPOND (appropriate activities to take action regarding a detected cybersecurity event), and RECOVER (appropriate activities to restore capabilities or services that are impaired due to a cybersecurity event).

The IRS's Cybersecurity Program was generally in alignment with FISMA requirements, but it was not fully effective due to program components not being at an acceptable maturity level. The Department of Homeland Security's scoring methodology defines "effective" as having maturity level 4, *Managed and Measurable*, or above.

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

The PROTECT function area rating was based on the metrics of four security program components: Configuration Management, which was at maturity level 2, *Defined*; Identity and Access Management, which was at maturity level 3, *Consistently Implemented*; Data Protection and Privacy, which was at maturity level 3, *Consistently Implemented*; and Security Training, which was at maturity level 4, *Managed and Measureable*. The end result for this function area was a maturity level 3, *Consistently Implemented*. The DETECT function area rating was based on the Information Security Continuous Monitoring metrics, which TIGTA deemed at maturity level 2, *Defined.*

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 will remain 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

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 24, 2019

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 2019 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act (Audit # 201920001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] (FISMA) evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2019. The Act requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. Our overall objective was to assess the effectiveness of the IRS information security program on a maturity model spectrum. This audit is included in our Fiscal Year 2019 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, 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, 128 Stat. 3073. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

Table of Contents

Background...Page 1

Results of Review ....Page 5

The Cybersecurity Program Was Generally Aligned With the Federal Information Security Modernization Act, but It Was Not Fully Effective in Two of the Five Cybersecurity Framework Function Areas...Page 5

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ....Page 33

Appendix II – Major Contributors to This Report......................................Page 35

Appendix III – Report Distribution List ....Page 36

Appendix IV – Information Technology Security-Related Audits Performed or Completed During the Fiscal Year 2019 Evaluation Period...Page 37

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
ICAM	Identity, Credential, and Access Management
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration

Background

The Federal Information Security Modernization Act of 2014,[1] commonly referred to as the FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA 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 another agency, a contractor, or other sources. 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 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. The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks.

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 contracted with Klynveld Peat Marwick Goerdeler, Limited Liability Partnership, to perform its FISMA evaluation on the non-IRS bureaus and has overall responsibility to combine the results for all the Treasury bureaus into one report for the OMB.

[1] Pub. L. No. 113-283, 128 Stat. 3703. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

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. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss.

Within the IRS, the Information Technology organization's Cybersecurity function is responsible for protecting taxpayer information and the electronic systems, services, and data from internal and external cybersecurity-related threats by implementing world class 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 2019 Inspector General FISMA Reporting Metrics

The Fiscal Year[2] 2019 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 2019 metrics represent a continuation of work that began in Fiscal Year 2016 to align the Inspector General metrics with the five cybersecurity function areas in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter referred to as the Cybersecurity Framework)[3] and transition the evaluation of all the function areas to the maturity model approach. The five Cybersecurity Framework function areas are as follows.

- IDENTIFY – Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.
- PROTECT – Develop and implement the appropriate safeguards to ensure delivery of critical services.
- DETECT – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- RESPOND – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- 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.

[2] Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.

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

Figure 1 shows the alignment of the eight security program components (or metric domains) to the five Cybersecurity Framework function areas.

Figure 1: Alignment of the NIST Cybersecurity Framework's Function Areas to the Fiscal Year 2019 Inspector General FISMA Metric Domains

Cybersecurity Framework's Function Areas	Fiscal Year 2019 Inspector General FISMA Metric Domains (Foundation Levels)
IDENTIFY	Risk Management
PROTECT	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
DETECT	Information Security Continuous Monitoring (ISCM)
RESPOND	Incident Response
RECOVER	Contingency Planning

Source: Fiscal Year 2019 Inspector General FISMA Reporting Metrics.

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum in which the foundation levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institute those policies and procedures. Maturity levels ranged 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 DHS's scoring methodology defines "effective" as having a maturity level 4, *Managed and Measurable*, or above.

Figure 2: Inspector General's Assessment Maturity Levels

Maturity Level	Description
Level 1: *Ad-hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measureable*	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 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.

Source: Fiscal Year 2019 Inspector General FISMA Reporting Metrics.

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 2019. This report covers the Fiscal Year 2019 FISMA evaluation period from July 1, 2018, through June 30, 2019. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Cybersecurity Program Was Generally Aligned With the Federal Information Security Modernization Act, but It Was Not Fully Effective in Two of the Five Cybersecurity Framework Function Areas

The IRS has 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 fully effective.

To determine the effectiveness of the Cybersecurity Program, we evaluated the maturity level of the program metrics specified by the DHS in the *Fiscal Year 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.3*. 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 the TIGTA and Government Accountability Office (GAO) audits. These audits, whose results were applicable to the FISMA metrics, were performed, completed, or contained open recommendations during the FISMA evaluation period, July 1, 2018, to June 30, 2019. See Appendix IV for a list of these audits. As shown in Figure 3, TIGTA rated three Cybersecurity Framework functions as "effective" and two as "not effective."

Figure 3: Maturity Levels by Function Area

Framework Foundation Function	Assessed Maturity Level	Effective?
IDENTIFY – Risk Management	Managed and Measurable (Level 4)	Yes
PROTECT –		
Configuration Management	Defined (Level 2)	No
Identity and Access Management	Consistently Implemented (Level 3)	
Data Protection and Privacy	Consistently Implemented (Level 3)	
Security Training	Managed and Measurable (Level 4)	
DETECT – ISCM	Defined (Level 2)	No
RESPOND – Incident Response	Managed and Measurable (Level 4)	Yes
RECOVER – Contingency Planning	Managed and Measurable (Level 4)	Yes

Source: TIGTA's evaluation of security program metrics that determined whether cybersecurity functions were rated "effective" or "not effective."

The Cybersecurity Framework function areas of IDENTIFY, RESPOND, and RECOVER were rated as "effective"

The Fiscal Year 2019 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 three function areas (IDENTIFY, RESPOND, and RECOVER) and their three security program components (Risk Management, Incident Response, and Contingency Planning) achieved the *Managed and Measurable* maturity level 4 and were deemed as "effective." The details of the results of our evaluation of the maturity levels are presented on pages 8, 27, and 29, respectively.

For the remaining two Cybersecurity Framework function areas, PROTECT and DETECT, we found four of their five security program components did not meet the *Managed and Measurable* maturity level for the reasons presented in the report. As a result, these two function areas were deemed as "not effective." The details of the results of our evaluation of the maturity levels are presented on pages 12, 17, 20, 22, and 25.

The Cybersecurity Framework function area of PROTECT was rated as "not effective"

The function area PROTECT consists of four security program components: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. Based on the Fiscal Year 2019 Inspector General FISMA Reporting Metrics, we found that the performance metrics for Security Training achieved a *Managed and Measurable* maturity level 4 and was therefore considered "effective." However, we determined that the security program components of Configuration Management was at a *Defined* maturity level 2. The security program component Identity and Access Management and Data Protection and Privacy were at a *Consistently Implemented* maturity level 3. As a result, these three program components were considered "not effective." Because three of the four program components were "not effective" with the overall result at a maturity level 3, we rated the entire PROTECT function area as "not effective."

In order for the IRS to meet an effective level for the Configuration Management, Data Protection and Privacy, and Identity and Access Management security program components, we believe it needs to improve on the following performance metrics.

- Specifically address the allocation of resources (people, processes, and technology) in a risk-based manner and accountability for effectively carrying out roles and responsibilities for configuration management.
- Ensure policies and procedures for maintaining baseline configurations or component inventories, secure configurations settings, flaw remediation and patching, and configuration change control are effectively implemented across the enterprise.

- Specifically address the allocation of resources in a risk-based manner for identity, credential, and access management (ICAM).
- Ensure that all nonprivileged and privileged accounts use strong authentication to access IRS information systems.
- Ensure that privileged accounts are provisioned, managed, and reviewed.
- Ensure that the encryption solutions are compliant with Federal Information Processing Standard Publication 140-2[4] on all of its remote access connections.
- Review and remove unnecessary Personally Identifiable Information collections on a regular basis.
- Fully implement all elements of the Data Loss Prevention solution, specifically those related to data at rest.
- Conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.
- Make updates to its privacy program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

The Cybersecurity Framework function area of DETECT was rated as "not effective"

Based on the Fiscal Year 2019 Inspector General FISMA Reporting Metrics, we found that the function area DETECT and its security program component, ISCM, met a *Defined* maturity level 2. In order for the IRS to meet an effective level for the ISCM program component, we believe it needs to improve on the following performance metrics.

- Continue to implement components to support Continuous Diagnostic and Mitigation.
- Ensure that adequate resources are allocated to cover ISCM positions.
- Continue to deploy automated capabilities to provide a view of the organizational security posture.
- Continue to implement its data collection/analysis tool and reporting system to support its ISCM dashboard for improved data collection, storage, analysis, retrieval, and reporting of performance measures.

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

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 will remain vulnerable to inappropriate and undetected use, modification, or disclosure.

TIGTA's response to the DHS's Fiscal Year 2019 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the Fiscal Year 2019 Inspector General FISMA Reporting Metrics are provided below. The metrics are based on Federal Government guidance and criteria, such as the NIST Special Publication 800-53[5] 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 when determining final ratings, as instructed by the Fiscal Year 2019 Inspector General FISMA Reporting Metrics.

Function Area 1: IDENTIFY – Risk Management

Maturity Level	Count
Ad-Hoc	**0**
Defined	**4**
Consistently Implemented	**1**
Managed and Measurable	**7**
Optimized	**0**
Function Rating: *Managed and Measurable* (Level 4)	

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: ***Managed and Measurable* (Level 4) –** The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.

2. To what extent does the organization use standard data elements/taxonomy[6] 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?

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

[6] 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: The IRS has not identified and documented all of its current system hardware components. TIGTA[7] not only reported that the firewall inventory and reporting tools were inaccurate and incomplete but also reported conflicting numbers of FISMA reportable firewalls. In addition, TIGTA[8] reported instances of hardware inventory issues, including unverified computers and uncontrolled hardware on the IRS's asset management system.

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 is still in the process of implementing systems for compiling a reliable software inventory. TIGTA[9] reported instances of software and associated licenses not being effectively managed and controlled.

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.

[7] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).

[8] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).

[9] TIGTA, Ref. No. 2019-20-005, *Management and Implementation of Information Technology Software Tools Needs Improvement* (Feb. 2019), and TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019).

Maturity Level: ***Managed and Measurable*** **(Level 4) –** The organization monitors and analyzes its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collects, analyzes, and reports information on the effectiveness of its risk management program. Data supporting risk management metrics are obtained accurately, consistently, and in a reproducible format.

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: ***Managed and Measurable*** **(Level 4) –** The organization's information security architecture is integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the information and communications technology supply chain and the organization's information systems.

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. Additionally, 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 Plans of Action and Milestones (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.

   Comments: We reviewed 52 weaknesses that the IRS identified during the annual testing of controls of the seven selected systems. Of those 52 weaknesses, we could not track 15 weaknesses to either existing or closed POA&Ms that supported effective remediation. In May 2019, the IRS issued a notification stating that POA&Ms will no longer be required for the general support system component weaknesses directly supporting an application for Fiscal Year 2020. This notification was in reference to 11 of the 52 weaknesses.

   In addition, we reviewed 63 POA&Ms that were closed in Fiscal Year 2019 related to the seven selected systems. Of the 63 POA&Ms that were closed, the IRS did not assess 14 closed POA&Ms during the Annual Security Controls Assessment process. We also found that 15 POA&Ms were closed without sufficient support that the weaknesses were corrected even though the IRS validated the closures through its closure verification process. Since being brought to its attention, the IRS provided additional evidence to support nine POA&M closures and has reopened three POA&Ms.

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: ***Defined*** **(Level 2) –** Policies and procedures for system-level risk assessments and security control selections are defined and communicated. In addition, the organization has developed a tailored set of baseline controls and provides guidance regarding acceptable risk assessment approaches.

   Comments: While the IRS has defined policies and procedures, it has not ensured that system risk assessments are consistently implemented. System authorization boundaries for a general support system and an application were not clearly defined.

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: ***Managed and Measurable*** **(Level 4) –** The organization employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.

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[10] clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements[11] 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)

[10] 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.

[11] 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 is obligated to meet.

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 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 has progressed in leveraging technology to manage risks, full implementation of additional advanced technologies will help improve the IRS's overall risk management capabilities.

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: ***Managed and Measurable* (Level 4) –** Based on the performance results for metrics 1 through 12, this function was evaluated at a maturity level 4, *Managed and Measurable*.

    Overall Risk Management Program Comments: The IRS risk management program is effective because it met the managed and measurable maturity level.

Function Area 2a: PROTECT – Configuration Management

Maturity Level	Count
Ad-Hoc	**0**
Defined	**5**
Consistently Implemented	**2**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: *Defined* (Level 2)	

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.

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

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 Lifecycle;[12] 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.

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.

[12] System Development Lifecycle 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.

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 systems we selected for the Fiscal Year 2019 FISMA evaluation did not maintain and have 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[13] and the GAO[14] reported instances of baseline configurations not being consistently implemented and 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 showed that five of the seven systems we selected for the Fiscal Year 2019 FISMA evaluation did not maintain secure configuration settings in accordance with IRS policy. In addition, least functionality controls were not fully in place for five of the seven systems, and flaw remediation controls were not fully in place for six of the seven systems. Furthermore, the IRS is awaiting the selection, implementation, and configuration of a software tool by DHS that will prevent unauthorized software program execution.

[13] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019); TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019); TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-005, *Management and Implementation of Information Technology Software Tools Needs Improvement* (Feb. 2019); TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018); TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018); TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018); and TIGTA, Ref. No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).

[14] GAO, GAO-19-474R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).

In addition, TIGTA[15] and the GAO[16] reported findings on systems that did not maintain secure configuration settings in accordance with agency policy. Further, the IRS is using a tool to assess configuration settings that are not Security Content Automation Protocol-compliant.[17] In addition, the GAO reported that the mainframe tools only test compliance with a limited subset of the agency's policies.

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. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws; testing software and firmware updates prior to implementation; installing relevant security updates and patches within organizational-defined time frames; and incorporating flaw remediation into the organization's configuration management processes.

    Comments: While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis. The IRS's annual security testing of systems reported that flaw remediation controls were not fully in place for six of the seven systems we selected for the Fiscal Year 2019 FISMA evaluation. Also, configuration change control was not fully in place for three of the seven systems. In addition, TIGTA[18] and the GAO[19] 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?

[15] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019); and TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018).

[16] GAO, GAO-19-150, *Financial Audit – IRS's Fiscal Years 2018 and 2017 Financial Statements* (Nov. 2018), and GAO, GAO-19-474R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).

[17] A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized use of security requirements.

[18] TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019); TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018); and TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018).

[19] GAO, GAO-19-474R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).

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.

Comments: This is the highest possible rating for this metric.

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,[20] 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 policies and procedures for managing configuration change control, these policies and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that three of the seven systems selected for the Fiscal Year 2019 FISMA evaluation had failed security controls related to configuration and change management practices. In addition, TIGTA[21] and the GAO[22] both 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 above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

[20] 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 lifecycle of an information system.

[21] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019); TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019); and TIGTA, Ref. No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).

[22] GAO, GAO-19-150, *Financial Audit – IRS's Fiscal Years 2018 and 2017 Financial Statements* (Nov. 2018), and GAO, GAO-19-474R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).

Overall Configuration Management Maturity Level: ***Defined* (Level 2)** – Based on the performance results for metrics 14 through 21, this function 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. The IRS indicated that it addresses the configuration management section in the Information Technology Security Program Plan dated July 2017.

Function Area 2b: PROTECT – Identity and Access Management

Maturity Level	Count
Ad-Hoc	**0**
Defined	**2**
Consistently Implemented	**5**
Managed and Measurable	**1**
Optimized	**1**
Function Rating: *Consistently Implemented* (Level 3)	

23. To what degree have the roles and responsibilities of ICAM 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.

    Comments: While the IRS has implemented key aspects of this metric, additional steps can be taken to ensure and document that risk-based decisions are carried out in a risk-based manner. The evidence provided by the IRS did not specifically address allocation of resources in a risk-based manner.

24. To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities?

    Maturity Level: ***Consistently Implemented* (Level 3) –** The organization is consistently implementing its ICAM strategy and is on track to meet milestones.

    Comments: The Treasury Enterprise ICAM office is preparing to roll out Phase 2 of DHS's Continuous Diagnostics and Mitigation program. The IRS uses the Treasury Enterprise ICAM to guide its ICAM initiatives.

25. To what degree have ICAM 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 ICAM, 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 ICAM policies, procedures, and processes to update the program.

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

26. To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate 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: ***Optimized* (Level 5) –** On a near real-time basis, the organization ensures that access agreements for privileged and non-privileged users are maintained, as necessary.

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

    Maturity Level: ***Consistently Implemented* (Level 3) –** The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

    Comments: While the IRS reported that 93 percent of its non-privileged users are required to use Personal Identity Verification cards to access the network, it also reported that only 29 of 135 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: ***Consistently Implemented* (Level 3) –** The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

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 29 of 135 internal systems are configured to require Personal Identity Verification cards.

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 managing privileged accounts, the IRS continues to experience control weaknesses related to privileged account management. TIGTA[23] reported that the IRS could not readily identify all individuals who had privileged access to its high-value asset components. In addition, TIGTA[24] reported that the IRS did not ensure that administrator accounts were compliant with IRS requirements for granting system access and did not review firewall administrator accounts semiannually.

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 on all of its remote access connections.

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?

[23] TIGTA, Ref. No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018)
[24] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).

Overall Identity and Access Management Maturity Level: ***Consistently Implemented* (Level 3)** – Based on the performance results for metrics 23 through 31, this function was evaluated at a maturity level 3, *Consistently Implemented.*

Overall Identity and Access Management Program Comments: The IRS Identity and Access Management Program is not effective because it did not meet the *Managed and Measurable* maturity level.

Function Area 2c: PROTECT – Data Protection and Privacy

Maturity Level	Count
Ad-Hoc	**0**
Defined	**2**
Consistently Implemented	**2**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: *Consistently Implemented* (Level 3)	

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

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

    Comments: The IRS did not provide sufficient evidence to show that it reviews and removes unnecessary Personally Identifiable Information collections on a regular basis. In addition, TIGTA[25] reported that the Privacy, Government Liaison, and Disclosure Office does not actively review Personally Identifiable Information collections on a regular basis to remove unnecessary Personally Identifiable Information.

34. To what extent has the organization implemented the following security controls to protect its Personally Identifiable Information and other agency sensitive data, as appropriate, throughout the data lifecycle (encryption of data at rest, encryption of data in transit,

[25] TIGTA, Ref. No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019).

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: While the IRS has defined policies and procedures, it has not ensured that the Data Loss Prevention software solution has been fully deployed, as previously reported by TIGTA.[26] Therefore, the IRS is not making full use of available tools to identify Personally Identifiable Information and other sensitive data for encryption. In addition, TIGTA[27] reported that data at rest related to Private Collection Agencies were not encrypted before or after transit in some cases.

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, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of Personally Identifiable Information. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology, audits its Domain Name Service records, and ensures the use of valid encryption certificates for its domains.

Comments: The IRS did not provide sufficient support that it conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

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

[26] TIGTA, Ref. No. 2019-20-049, *The First Phase of the Data Loss Prevention Solution Is Working As Intended, but the Remaining Phases Continue to Experience Delays* (Aug. 2019).

[27] TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

topics should include, as appropriate: responsibilities under the Privacy Act of 1974[28] and E-Government Act of 2002;[29] consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents; and data collections and use requirements.)

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

Comments: The IRS has not provided sufficient evidence to support that it makes updates to its privacy program based on statutory, regulatory, mission, program, business process, and information system requirements and/or 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: ***Consistently Implemented* (Level 3) –** Based on the performance results for metrics 33 through 37, this function was evaluated at a maturity level 3, *Consistently Implemented.*

Overall Data Protection and Privacy Program Comments: The IRS data protection and privacy program is not effective because it did not meet the *Managed and Measurable* maturity level.

Function Area 2d: PROTECT – Security Training

Maturity Level	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**2**
Managed and Measurable	**4**
Optimized	**0**
Function Rating: *Managed and Measurable* (Level 4)	

[28] Privacy Act of 1974, 5 U.S.C. § 552a (2013).
[29] Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat 2899.

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

    Comments: The IRS did not provide evidence to support *Managed and Measurable.*

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: ***Consistently Implemented*** **(Level 3) –** The organization has conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.

    Comments: The IRS did not provide evidence to support *Managed and Measurable.*

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 email 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, and 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, and/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, and/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 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.

Function Area 3: DETECT – Information Security Continuous Monitoring

Maturity Level	Count
Ad-Hoc	**0**
Defined	**3**
Consistently Implemented	**2**
Managed and Measurable	**0**
Optimized	**0**
Function Rating: *Defined* (Level 2)	

46. To what extent does the organization utilize an information security continuous monitoring (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: While the IRS has developed and communicated its ISCM strategy and procedures across its enterprise, it has not provided us with sufficient evidence to meet the *Managed and Measureable* maturity levels for monitoring and analyzing qualitative and quantitative performance measures on its effectiveness of its ISCM strategy.

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; analyzing ISCM data; reporting findings; and reviewing and updating the ISCM strategy. (Note: The overall maturity level should take into consideration the maturity of question 49.)

    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: The IRS is waiting on the Department of the Treasury to address DHS Binding Operational Directive. Meanwhile, the IRS indicated that it issued a memorandum in September 2019 requiring any DHS Binding Operational Directive to take precedence over existing policy. In addition, the IRS is working to implement the components to support

Continuous Diagnostics and Mitigation. Further, based on the maturity level of metric 49, the IRS does not meet *Consistently Implemented*.

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 defined and communicated the structure of its ISCM across the organization. OMB directives require that all employees who spend at least 20 percent of their time on cybersecurity activities be assigned work roles per the National Initiative on Cybersecurity Education framework. IRS management assigned over 90 percent of its Cybersecurity employees to National Initiative on Cybersecurity Education framework roles. However, it has not ensured that adequate resources are allocated to cover positions responsible for ISCM roles and responsibilities. TIGTA[30] reported that the IRS's limited resources placed additional burden on asset management (which is part of the ISCM program plan).

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

    Maturity Level: ***Defined* (Level 2) –** The organization has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.

    Comments: While the IRS has processes in place to conduct security control assessments, they are generally manual in nature. The IRS indicated that it is deploying automated capabilities, but they are not fully in place to provide a view of the organizational security posture for consideration on granting system authorization.

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

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

    Comments: 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. The IRS indicated that it is working to improve the

[30] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).

Continuous Diagnostic and Mitigation dashboard to ensure that current data is flowing from the sensor tools into the dashboard correctly.

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

Overall ISCM Maturity Level: ***Defined* (Level 2) –** Based on the performance results for metrics 46 through 50, this function was evaluated at a maturity level 2, *Defined.*

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

Function Area 4: RESPOND – Incident Response

Maturity Level	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**2**
Managed and Measurable	**4**
Optimized	**1**
Function Rating: *Managed and Measurable* (Level 4)	

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 53–58.)

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 to support that it ensures 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.

Comments: This is the highest possible rating 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. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems.

Comments: This is the highest possible rating for this metric.

55. How mature are the organization' 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 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 US-CERT,[31] law enforcement, the agency's 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 Measureable* maturity level.

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.

Comments: This is the highest possible rating for this metric.

[31] US-CERT is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security.

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 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 Measureable* maturity level.

Function Area 5: RECOVER – Contingency Planning

Maturity Level	Count
Ad-Hoc	**0**
Defined	**1**
Consistently Implemented	**2**
Managed and Measurable	**4**
Optimized	**0**
Function Rating: *Measurable and Measurable* (Level 4)	

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

    Comments: While the IRS met consistently implemented, the IRS did not provide evidence to show that resources are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities and support to ensure that 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 62–66.)

    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 incorporates the results of organizational and system level business impact analyses into strategy and plan development efforts 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.

    Comments: This is the highest possible rating for the 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,[32] 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 processes, strategies, and technologies for information system backup and storage (including use of alternate storage and processing sites) have been defined, it has not ensured that they are consistently implemented. The IRS's annual security testing of organizational common controls reported that it does not perform backup testing according to IRS standards.

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 obtained accurately, consistently, and in a reproducible format.

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?

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

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

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

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 2019 Inspector General FISMA Reporting Metrics that pertain to eight security program components.

As instructed in the reporting metric document, we determined the overall rating for each of the eight domains by a simple majority rule, whereby the most frequent 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, then the domain rating is *Managed and Measurable*. However, we also considered agency-specific factors when determining final ratings, as instructed by the Fiscal Year 2019 Inspector General FISMA Reporting Metrics. In addition, as instructed in the reporting metric document, we were required to provide comments explaining the rational for why a given metric was rated lower than a maturity level 4, *Managed and Measureable*. The Treasury Office of Inspector General will combine our results for the IRS with its results for the non-IRS bureaus and input the combined results into Cyberscope.[1]

I. Determine the effectiveness of the Risk Management program.

II. Determine the effectiveness of the Configuration Management program.

III. Determine the effectiveness of the Identity and Access Management program.

IV. Determine the effectiveness of the Data Protection and Privacy program.

V. Determine the effectiveness of the Security Training program.

VI. Determine the effectiveness of the ISCM program.

VII. Determine the effectiveness of the Incident Response program.

VIII. Determine the effectiveness of the Contingency Planning program.

We 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 follows the selection methodology that the Treasury Office of Inspector General defined for the Department of the Treasury as a whole. We used the system inventory contained within the Treasury FISMA Inventory Management System of general support systems, major applications, and minor

[1] Cyberscope, which was implemented in Fiscal Year 2009, is the Federal repository for collecting FISMA data.

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.

We also considered the results of TIGTA audits performed or completed during the Fiscal Year 2019 FISMA evaluation period, as listed in Appendix IV, as well as audit reports from the GAO that contained results applicable to the FISMA metrics.

Appendix II

Major Contributors to This Report

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
George Franklin, Senior Auditor
Bret Hunter, Senior Auditor
Steven Stephens, Senior Auditor
Suzanne Westcott, Senior Auditor
Esther Wilson, Senior Auditor
Linda Nethery, Senior Information Technology Specialist
Thomas Martin, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Director, Enterprise Audit Management

Appendix IV

Information Technology Security-Related Audits Performed or Completed During the Fiscal Year 2019 Evaluation Period

1. TIGTA, Ref. No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).
2. TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018).
3. TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).
4. TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
5. TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018).
6. GAO, GAO-19-150, *Financial Audit – IRS's Fiscal Years 2018 and 2017 Financial Statements* (Nov. 2018).
7. TIGTA, Ref. No. 2019-20-005, *Management and Implementation of Information Technology Software Tools Needs Improvement* (Feb. 2019).
8. TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019).
9. GAO, GAO-19-474R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).
10. TIGTA, Ref. No. 2019-20-049, *The First Phase of the Data Loss Prevention Solution Is Working As Intended, but the Remaining Phases Continue to Experience Delays* (Aug. 2019).
11. TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019).
12. TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).
13. TIGTA, Ref. No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019).